McAfee Total Protection for Endpoint Handbuch zur Testversion



Inhaltsverzeichnis

Einführung in McAfee Total Protection for Endpoint

Willkommen bei McAfee® Total Protection® for Endpoint. Diese Lösung enthält die beste und umfassendste McAfee-Sicherheit für Endpunkte, E-Mail, Internet und Daten. Im Vergleich zum Kauf und der Verwaltung unterschiedlicher Sicherheitskomponenten von mehreren Anbietern spart McAfee Total Protection for Endpoint Zeit und Geld und bietet einen leistungsfähigeren, integrierten Schutz gegen bekannte und unbekannte Bedrohungen für Unternehmen.

Dieses Handbuch ist so organisiert, dass Sie McAfee Total Protection for Endpoint in einer Pilot-Umgebung testen können, die aus einem ePolicy Orchestrator®-Server (ePO™) und mehreren Client-Computern besteht. Das Handbuch behandelt die grundlegenden Schritte zum schnellen Installieren von ePolicy Orchestrator, zum Konfigurieren grundlegender Richtlinien und Tasks sowie zum Ausbringen der folgenden McAfee-Produkte zum Schutz von Clients:

- VirusScan® Enterprise 8.7i
- AntiSpyware Enterprise 8.7
- Host Intrusion Prevention 7.0
- SiteAdvisor® Enterprise Plus 2.0
- GroupShield® 7.0

Dieses Handbuch bietet praxisnahe Beispiele für Schritte, die Sie bei einer realen Ausbringung vornehmen müssen. Es behandelt nicht jedes mögliche Ausbringungsszenario und nicht alle enthaltenen Funktionen. Vollständige Informationen zu allen Aspekten der Produkte, die in Total Protection for Endpoint enthalten sind, finden Sie in den jeweiligen Produkthandbüchern.

Die vollständige Produktdokumentation ist in der McAfee KnowledgeBase verfügbar.

Klicken Sie unter **Self Service** (Online-Support) auf **Read Product Documentation** (Produktdokumentation lesen), wählen Sie ein Produkt und dessen Version und anschließend das gewünschte Dokument aus.

Produktbeschreibungen

Die Produkte in Total Protection for Endpoint sind in folgende Kategorien gruppiert:

- Verwaltungslösung
- Endpunkt-Schutz
- E-Mail-Server-Schutz

Verwaltungslösung

Total Protection for Endpoint bietet folgende Produkte für eine Verwaltungslösung an.

Produkt	Beschreibung
McAfee ePolicy Orchestrator	ePolicy Orchestrator ist die branchenweit führende Sicherheitsverwaltungslösung für Systeme in einem Unternehmen. Sie

Produkt	Beschreibung
	bietet einen koordinierten, proaktiven Schutz vor böswilligen Bedrohungen und Angriffen. ePolicy Orchestrator vereint unerreichte globale Richtlinienkontrolle mit einem einzelnen Agenten und einer zentralen Konsole mit benutzerdefinierter Berichterstellung zur einfachen Verwaltung der Systemsicherheitsumgebung.
McAfee Agent	McAfee Agent ist das clientseitige Framework, das die Sicherheitsverwaltungsinfrastruktur von McAfee unterstützt. Es gewährleistet sichere Kommunikation zwischen den verwalteten Produkten und ePolicy Orchestrator sowie lokale Dienste für verwaltete Produkte. Als Framework ermöglicht McAfee Agent es verwalteten Produkten, ihre Richtlinien zu erzwingen und dabei erweiterbare Dienste und Funktionen anzubieten. Dazu gehören Protokollierung, Kommunikation und Richtlinienspeicherung.

Endpunkt-Schutz

Total Protection for Endpoint bietet folgende Produkte zum Endpunkt-Schutz an.

Produkt	Beschreibung
McAfee VirusScan® Enterprise 8.7i	VirusScan Enterprise, ein vertrauenswürdiger Name auf dem Gebiet der Sicherheit, ist führend bei fortgeschrittenem, proaktivem Schutz von PCs und Servern. Bei einem Ausbruch vertrauen Unternehmen auf die wichtigsten Funktionen von VirusScan Enterprise. Dazu gehören: Säubern des Speichers, der Registrierung und der Dateien, Entfernen von Rootkits sowie Verhindern der Ausbreitung von schädlichem Code auf andere Systeme. VirusScan Enterprise enthält auch Funktionen zum Schutz vor Viren und Eindringungsversuchen sowie zum Schutz der Firewall vor bekannten und unbekannten Angriffen.
McAfee AntiSpyware Enterprise 8.7	AntiSpyware Enterprise Module, die führende Anti-Spyware-Lösung für Unternehmen, kann mithilfe von On-Access-Scans potenziell unerwünschte Programme (PUPs) identifizieren, proaktiv blockieren und sicher entfernen und gewährleistet auf diese Weise optimale geschäftliche Verfügbarkeit. McAfee AntiSpyware Enterprise Module, das mit ePolicy Orchestrator zentral verwaltetet wird, integriert sich nahtlos in VirusScan Enterprise und verringert Störungen aufgrund von Bedrohungen und PUPs.
McAfee Host Intrusion Prevention 7.0	Host Intrusion Prevention kann dank der Kombination von Signatur- und verhaltensbasiertem Schutz mit einer Systemfirewall Eindringungen überwachen und blockieren. Die Abschirmung Ihrer Ressourcen verbessert die Verfügbarkeit, Vertraulichkeit und Integrität Ihrer Geschäftsprozesse. Mit einem einzelnen Agenten wird das Ausbringen, Konfigurieren und Verwalten vereinfacht, und das Ausbringen von Patches muss seltener und weniger dringlich erfolgen.
McAfee SiteAdvisor® Enterprise Plus 2.0	Mit SiteAdvisor Enterprise Plus können Ihre Mitarbeiter das Internet sicher benutzen und durchsuchen, da Spyware, Adware, Phishing-Betrug und ähnliche Bedrohungen blockiert werden. Durch die Integration in McAfee-Lösungen wird der umfassende Schutz mithilfe der Technologie von SiteAdvisor Enterprise noch um Internetsicherheit erweitert und die Benutzer werden auf diese Weise vor Online-Bedrohungen geschützt.

E-Mail-Server-Schutz

Total Protection for Endpoint bietet folgende Produkte zum E-Mail-Server-Schutz an.

Produkt	Beschreibung
McAfee GroupShield® 7.0	GroupShield schützt E-Mails und andere Dokumente, wenn sie den Microsoft Exchange- und Lotus Domino-Server erreichen oder verlassen. GroupShield scannt proaktiv auf Viren, verwaltet automatisch Ausbrüche und verhindert, dass böswilliger Code Ihre Systeme schädigt. Der

Produkt	Beschreibung
	Inhaltsfilter von GroupShield blockiert oder isoliert Nachrichten, die bestimmte Wörter und Begriffe enthalten und Inhaltsregeln verletzen.
McAfee Anti-Spam for GroupShield 7.0	Anti-Spam for GroupShield blockiert Spam auf Ihren Microsoft Exchange- und Lotus Domino-E-Mail-Servern. Auf diese Weise verbessert sich die Produktivität Ihrer Mitarbeiter. Gleichzeitig wird verhindert, dass vertrauliche Daten aufgrund von Phishing-Betrug kompromittiert werden. Anti-Spam wird in McAfee GroupShield integriert und verringert den Ressourcenverbrauch auf ausgelasteten E-Mail-Servern.

Wenn Sie bereit sind, Produkte in Ihrer Umgebung auszubringen (z. B. VirusScan Enterprise oder Host Intrusion Prevention), verwenden Sie ePolicy Orchestrator und McAfee Agent zum Durchführen der Ausbringung und von Aktualisierungen. McAfee empfiehlt, den Workflow in den folgenden Abschnitten für die Lösung zu verwenden.

Vor der Installation

Prüfen Sie vor dem Einrichten von McAfee Total Protection for Endpoint, ob alle Komponenten die nachfolgend aufgeführten minimalen Systemanforderungen erfüllen.

Serveranforderungen

Minimale Hardware- und Netzwerkanforderungen

- **Verfügbarer Speicherplatz** – Mindestens 1 GB; 2 GB empfohlen.
- **RAM** – 1 GB verfügbar; 2-4 GB empfohlen.
- **Prozessor** – Intel Pentium III-Klasse oder höher; 1 GHz oder höher.
- **Monitor** – 1024 x 768, 256 Farben, VGA-Monitor.
- **Netzwerkkarte** – 100 MB oder höher.
- **Dateisystem** – NTFS-Partition (NT-Dateisystem) empfohlen.
- **IP-Adresse** – Für ePolicy Orchestrator-Server werden statische IP-Adressen empfohlen.

Softwareanforderungen

- **Server-Betriebssysteme**
  - Windows 2000 Server mit Service Pack 4 oder höher
  - Windows 2000 Advanced Server mit Service Pack 4 oder höher
  - Windows Server 2003 Enterprise mit Service Pack 1 oder höher
  - Windows Server 2003 Standard mit Service Pack 1 oder höher
  - Windows Server 2003 Web mit Service Pack 1 oder höher
  - Windows Server 2003 R2 Enterprise
  - Windows Server 2003 R2 Standard
  - Windows Server 2008
- **Browser**
  - Microsoft Internet Explorer 6.0 mit Service Pack 1 oder höher.
  - Microsoft Internet Explorer 7.0.
  - Wenn Sie einen Proxy verwenden, umgehen Sie wie folgt den Proxyserver:

  1. Wählen Sie in Internet Explorer im Menü **Extras** die Option **Internetoptionen** aus.
  2. Klicken Sie auf die Registerkarte **Verbindungen**, und klicken Sie dann auf **LAN-Einstellungen**.
  3. Aktivieren Sie **Proxyserver für LAN verwenden**, und aktivieren Sie dann für lokale Adressen **Proxyserver für lokale Adressen umgehen**.

4 Klicken Sie auf **OK**, bis das Dialogfeld **Internetoptionen** geschlossen ist.

- **Domänen-Controller** – Mit ePolicy Orchestrator können Sie Systeme in einer Arbeitsgruppe oder einer Windows-Domäne verwalten. In den Installationsanweisungen weiter unten wird Letzteres behandelt, wofür der Server Mitglied der Windows-Domäne sein muss. Entsprechende Anweisungen finden Sie in der Dokumentation des Microsoft-Produkts.
- **Sicherheitssoftware**
  - Installieren bzw. aktualisieren Sie die Antivirensoftware auf dem ePolicy Orchestrator-Server, und führen Sie einen Scan durch.

    VORSICHT: Wenn VirusScan Enterprise 8.5i oder 8.7i auf dem System ausgeführt wird, auf dem Sie ePolicy Orchestrator installieren, müssen Sie sicherstellen, dass die VSE-Zugriffsschutzregeln während des ePO-Installationsvorgangs deaktiviert sind, da die Installation andernfalls fehlschlägt.
  - Installieren bzw. aktualisieren Sie die Firewall-Software auf dem ePolicy Orchestrator-Server.

Erwägungen zur Datenbank

Vor dem Installieren von ePO muss bereits eine Datenbank installiert sein. Standardmäßig wird während des Setup die SQL Server 2005 Express-Datenbank und anschließend ePolicy Orchestrator auf demselben Server installiert. Beachten Sie, dass ePO auch mit anderen Datenbanken verwendet werden kann, z. B. MSDE 2000, SQL 2000 oder SQL 2005 Server. Weitere Informationen finden Sie im *ePO 4.0-Installationshandbuch*.

Sonstige Softwareanforderungen

Software	Anmerkungen
MSXML 6.0	Wenn diese Software nicht zuvor installiert wurde, wird sie vom Installations-Assistenten automatisch installiert.
Internet Explorer 6 SP1 oder höher	Sie müssen diese Software herunterladen und installieren.
.NET Framework 2.0	Wenn diese Software nicht zuvor installiert wurde, wird sie vom Installations-Assistenten automatisch installiert.
MDAC 2.8	Wenn diese Software nicht zuvor installiert wurde, wird sie vom Installations-Assistenten automatisch installiert.
SQL Server 2005 Backward Compatibility	Wenn diese Software nicht zuvor installiert wurde, wird sie vom Installations-Assistenten automatisch installiert.

Unterstützte Sprachversionen von Betriebssystemen

Diese McAfee Total Protection for Endpoint-Version funktioniert mit folgenden Sprachversionen der entsprechenden unterstützten Betriebssysteme:

- Chinesisch (Vereinfacht)
- Chinesisch (Traditionell)
- Englisch
- Französisch (Standard)
- Koreanisch
- Spanisch
- Deutsch (Standard)
- Japanisch

Einrichten der McAfee Total Protection for Endpoint-Suite

Dieser Abschnitt führt Sie durch die Installation der McAfee Total Protection for Endpoint-Suite mit den Standardoptionen. Das Installationsprogramm der McAfee Total Protection for Endpoint-Suite richtet den ePO-Server ein und checkt die Software der Endpunkt-Produkte in das ePO-Repository ein.

Vorgehensweise

1. Laden Sie McAfee Total Protection for Endpoint von der offiziellen McAfee-Webseite in ein temporäres Verzeichnis auf dem ePO-Server oder dem zur Verwaltung vorhergesehenen Server herunter, und extrahieren Sie die Software dort.
2. Doppelklicken Sie auf **Setup.exe**. Die Seite **Willkommen beim Setup von McAfee ePolicy Orchestrator für Total Protection for Endpoint** wird angezeigt.
3. Klicken Sie auf **Weiter**. Die Seite **Test** wird angezeigt.
4. Klicken Sie auf **OK**. Die Seite **Endbenutzer-Lizenzvertrag** wird angezeigt.
5. Akzeptieren Sie den Endbenutzer-Lizenzvertrag, und klicken Sie dann auf **OK**. Die Seite **Software zum Bewerten auswählen** wird mit den folgenden standardmäßig aktivierten Optionen angezeigt:
   - Basisinstallation
   - Host Intrusion Prevention
   - GroupShield für E-Mail-Server
6. Klicken Sie auf **Weiter**. Die Seite **Administratorinformationen festlegen** wird angezeigt.
7. Geben Sie den Benutzernamen und das Kennwort für das ePolicy Orchestrator-Administratorkonto ein, und klicken Sie dann auf **Weiter**. Die Seite **Setup-Typ auswählen** wird angezeigt.

   HINWEIS: Sie müssen dieselben Anmeldeinformationen später zum Anmelden bei ePolicy Orchestrator verwenden.
8. Wählen Sie **Standard** aus, um ePolicy Orchestrator und Microsoft SQL 2005 Express mit den Standardeinstellungen am Standardspeicherort zu installieren, und klicken Sie dann auf **Weiter**. Ein Bestätigungsdialogfeld wird angezeigt.
9. Klicken Sie auf **OK**, um Microsoft SQL 2005 Express zu installieren. Die Seite **Datenbankinformationen festlegen** wird angezeigt.
10. Geben Sie den Kontotyp und die Authentifizierungsdetails an, die der ePolicy Orchestrator-Server zum Zugriff auf die Datenbank verwendet.
    - Wählen Sie im Dropdownfeld **Anmeldeinformationen für Datenbankserver** die Windows-Domäne aus, geben Sie den Namen und das Kennwort für den

Domänenbenutzer ein, und klicken Sie dann auf **Weiter**. Die Seite **Kopieren der Dateien wird gestartet** wird angezeigt.

HINWEIS: Die Windows-Authentifizierung ist aktiviert, da SQL Express standardmäßig keine SA-Authentifizierung erlaubt.

11 Klicken Sie auf **Weiter**, um mit der Installation zu beginnen. Die Seite **InstallShield Wizard abgeschlossen** wird mit den folgenden standardmäßig aktivierten Optionen angezeigt:

- Aktivieren Sie **Ja, ich möchte die README-Datei anzeigen**, um die Readme-Datei anzuzeigen.
- Aktivieren Sie **Ja, ich möchte McAfee ePolicy Orchestrator jetzt starten**, um die Benutzeroberfläche von ePolicy Orchestrator zu starten.

HINWEIS: Falls ein Konflikt mit den Standard-Portnummern vorliegen sollte, werden Sie während des Installationsvorgangs aufgefordert, diese zu ändern.

12 Klicken Sie auf **Fertig stellen**.

Anmelden bei ePolicy Orchestrator

Gehen Sie wie nachfolgend beschrieben vor, um sich bei ePolicy Orchestrator anzumelden. Sie benötigen dazu gültige Anmeldeinformationen.

Vorgehensweise

1. Öffnen Sie zum Starten von ePolicy Orchestrator einen Internet-Browser, und wechseln Sie zur URL des Servers (**z. B.:** *https://<Servername>:8443*). Das Dialogfeld **Anmelden bei ePolicy Orchestrator-Server** wird angezeigt.

   HINWEIS: Sie können ePolicy Orchestrator auch mit einem Doppelklick auf das Desktop-Symbol von McAfee ePolicy Orchestrator starten.

2. Geben Sie den **Benutzernamen** und das **Kennwort** für ein gültiges Konto ein, das Sie im Abschnitt *Einrichten der McAfee Total Protection for Endpoint-Suite* in *Schritt 7* erstellt haben.

   HINWEIS: Kennwörter berücksichtigen Groß- und Kleinschreibung.

3. Wählen Sie die **Sprache** aus, in der die Software angezeigt werden soll.
4. Klicken Sie auf **Anmelden**.

Einrichten des ePolicy Orchestrator-Servers

Das ePolicy Orchestrator-Repository ist der zentrale Speicherort für alle Produktinstallationen, Aktualisierungen und Signaturpakete von McAfee. Durch den modularen Aufbau von ePolicy Orchestrator können neue Produkte als *Erweiterungen* hinzugefügt werden. Dazu gehören neue oder aktualisierte Versionen von McAfee-Produkten, z. B. VirusScan Enterprise, und Nicht-McAfee-Produkte von McAfee-Partnern. *Pakete* sind Komponenten, die in das Master-Repository eingecheckt und dann auf Client-Systeme ausgebracht werden.

Informationen zu Erweiterungen und Paketen finden Sie in den folgenden Themen des *ePolicy Orchestrator-Produkthandbuchs*:

- *Erweiterungen und ihre Funktion*
- *Ausbringungspakete für Produkte und Aktualisierungen*

Entsprechend Ihrer Auswahl bei der Installation wurde der Total Protection for Endpoint-Client zum ePO-Master-Repository hinzugefügt. Wechseln Sie zum Überprüfen der Installation zum Master-Repository.

Konfigurieren eines Repository-Abruf-Tasks

Damit ePolicy Orchestrator Ihre Client-Systeme auf dem neuesten Stand halten kann, müssen Sie einen *Repository-Abruf-Task* konfigurieren, der in festgelegten Intervallen Aktualisierungen von einer McAfee-Webseite (HTTP oder FTP) abruft.

HINWEIS: Während der Installation wurde automatisch ein Repository-Abruf-Task erstellt.

Vorgehensweise

Gehen Sie wie nachfolgend beschrieben vor, um einen Repository-Abruf-Task zu erstellen, der die Client-Software hinzufügt und aktualisiert.

1. Wechseln Sie zu **Automatisierung |** Server-Tasks.
2. Suchen Sie in der Liste den Task "Master-Repository aktualisieren", und klicken Sie in der Spalte **Aktionen** auf **Bearbeiten**, um den Generator für Server-Tasks zu öffnen.
3. Legen Sie auf der Seite **Beschreibung** den **Planungsstatus** auf **Aktiviert** fest, und klicken Sie dann auf **Weiter**.
4. Auf der Seite **Aktionen** befindet sich direkt unter der Seitenbeschreibung ein grauer Balken mit der Beschriftung **1**. Wählen Sie in der Dropdownliste den Eintrag **Repository-Abruf** aus.
5. Aktivieren Sie **Vorhandenes Paket in den Zweig "Vorherige" verschieben**, und klicken Sie dann auf **Weiter**.

   HINWEIS: Durch Aktivieren dieser Option kann ePolicy Orchestrator die Signaturdateien von mehr als einem Tag verwalten. Wenn der nächste Abruf-Task ausgeführt wird, werden die aktuellen Aktualisierungen in das Verzeichnis **Vorherige** auf dem Server verschoben. Auf diese Weise können Sie Aktualisierungen bei Bedarf zurücksetzen.

6 Wählen Sie auf der Seite **Plan** aus, wann ePolicy Orchestrator auf der McAfee-Webseite nach Aktualisierungen suchen soll.
   - Wählen Sie **Täglich** und **Kein Enddatum** aus.
   - Legen Sie für **Plan** die Option **zwischen 9:00 und 23:00** fest.
   - Wählen Sie für **Alle** zwei oder drei Stunden aus.

   TIPP: McAfee empfiehlt, mehrmals täglich nach Aktualisierungen zu suchen, damit Sie wirklich über die aktuellsten Inhalte verfügen.

7 Klicken Sie auf **Weiter**.
8 Klicken Sie auf der Seite **Zusammenfassung** auf **Speichern**. Die Konsole kehrt zur Seite **Server-Tasks** zurück.
9 Suchen Sie den Task "Master-Repository aktualisieren", und klicken Sie in der Spalte **Aktionen** auf **Ausführen**. Es wird sofort nach Aktualisierungen gesucht, und das Server-Task-Protokoll wird geöffnet.

Überprüfen des Status des Abruf-Tasks

Im Server-Task-Protokoll können Sie den Status des Abruf-Tasks von McAfee anzeigen. Gehen Sie wie nachfolgend beschrieben vor, um zu überprüfen, ob der Task "Master-Repository aktualisieren" das Abrufen von Aktualisierungen von der McAfee-Webseite abgeschlossen hat.

Vorgehensweise

1 Wechseln Sie zu **Berichterstellung |** Server-Task-Protokoll.
2 Suchen Sie in der Task-Liste den Task "Master-Repository aktualisieren".
3 Der Task ist abgeschlossen, wenn in der Spalte **Status** die Meldung **Abgeschlossen** angezeigt wird.

Hinzufügen von Systemen zum Verwalten

Die Systemstruktur von ePolicy Orchestrator organisiert verwaltete Systeme in Einheiten, um sie zu überwachen, Richtlinien zuzuordnen, Tasks zu planen und Aktionen auszuführen. Diese Einheiten werden als *Gruppen* bezeichnet, die von globalen Administratoren oder Benutzern mit den entsprechenden Berechtigungen erstellt und verwaltet werden. Sie können sowohl Systeme als auch andere Gruppen enthalten. Bevor Sie Endpunkt-Richtlinien für Client-Systeme in Ihrem Netzwerk verwalten können, müssen Sie diese Systeme zur Systemstruktur hinzufügen.

Es gibt verschiedene Methoden zum Organisieren und Auffüllen der Systemstruktur:

- Manuelles Strukturieren der Systemstruktur durch Erstellen eigener Gruppen und Hinzufügen einzelner Systeme.
- Synchronisieren mit einem Active Directory oder einer NT-Domäne als Quelle für Systeme. Bei Verwendung von Active Directory wird durch die Synchronisierung auch eine Systemstruktur bereitgestellt.
- Erstellen von eigenen Gruppen auf der Basis von IP-Bereichen oder Subnetzen. Dies wird als *kriterienbasierte Sortierung* bezeichnet.
- Importieren von Gruppen und Systemen aus einer Textdatei.

Im in diesem Abschnitt beschriebenen Workflow wird für den Test eine einfache Struktur manuell erstellt. Während diese Methode beim Ausbringen von ePolicy Orchestrator in einem realen Netzwerk möglicherweise zu langsam ist, eignet sie sich gut zum Hinzufügen weniger Systeme in einem Testnetzwerk. Die anderen Methoden können Sie ausprobieren, wenn Sie sich mit ePolicy Orchestrator vertraut gemacht haben.

Erstellen von Systemstrukturgruppen

Gehen Sie wie nachfolgend beschrieben vor, um Gruppen zur Systemstruktur hinzuzufügen. Erstellen Sie für diese Übung zwei Gruppen: *Server* und *Workstations*.

1. Wechseln Sie zu **Systeme |** Systemstruktur, und klicken Sie dann in der Menüleiste auf **Gruppe**.
2. Markieren Sie **Eigene Organisation**, und klicken Sie dann auf **Neue Untergruppe**.
3. Geben Sie Testgruppe ein, und klicken Sie dann auf **OK**. Die neue Gruppe wird in der Systemstruktur angezeigt.
4. Markieren Sie **Testgruppe**, und klicken Sie auf **Neue Untergruppe**. Geben Sie Server ein, und klicken Sie auf **OK**.
5. Wiederholen Sie Schritt 4, geben Sie nun aber Workstations als Gruppennamen ein. Wechseln Sie zurück zur Seite **Gruppe**, und markieren Sie **Testgruppe**. Ihre Gruppen **Server** und **Workstations** werden nun auf der Seite **Gruppe** angezeigt. Sie sind in der Reihenfolge sortiert, in der Sie die Gruppen erstellt haben.

Hinzufügen von Systemen zu Systemstrukturgruppen

Gehen Sie wie nachfolgend beschrieben vor, um einige Testsysteme manuell zur ePO-Systemstruktur hinzuzufügen.

1 Markieren Sie in der Systemstruktur die Gruppe **Workstations**, und klicken Sie auf **Neue Systeme**.
2 Wählen Sie unter **Systeme auf diese Weise hinzufügen** die Option **Systeme zur aktuellen Gruppe hinzufügen, aber keine Agenten ausbringen** aus.
3 Geben Sie bei **Hinzuzufügende Systeme** den NetBIOS-Namen für die einzelnen Systeme in das Textfeld ein, und trennen Sie diese mit Kommas, Leerzeichen oder Zeilenumbrüchen. Sie können auch auf **Durchsuchen** klicken, um Systeme auszuwählen.
4 Stellen Sie sicher, dass das Kontrollkästchen in der Zeile **Systemstruktursortierung** deaktiviert ist.
5 Klicken Sie auf **OK**.
6 Wiederholen Sie diese Schritte bei Bedarf, um Systeme zur Gruppe **Server** hinzuzufügen.

Organisieren neuer Systeme in den Gruppen

Nachdem Sie die Schritte in den vorhergehenden Abschnitten ausgeführt haben, befinden sich nun mehrere Gruppen und Systeme in der Systemstruktur. In einer realen Produktionsumgebung kontaktieren neue Systeme den ePolicy Orchestrator-Server und müssen in die Systemstruktur eingeordnet werden. Dies ist der Fall, wenn Sie McAfee Agent mithilfe von Rogue System Detection oder einem anderen Verfahren auf neuen Systemen installiert haben. Dabei werden die Systeme in die Sammelgruppe aufgenommen.

ePolicy Orchestrator verfügt über eine leistungsstarke Gruppensortierungsfunktion, mit der Sie Regeln dafür festlegen können, wie sich die Systeme beim ersten Kontakt mit dem ePO-Server in die Systemstruktur einordnen. Ausführliche Informationen zu dieser Funktion finden Sie im *ePolicy Orchestrator 4.0-Produkthandbuch* unter Kriterienbasierte Sortierung.

In dieser Übung erstellen Sie eine auf Tags basierende Systemsortierungsregel. ePolicy Orchestrator erstellt zwei Standard-Tags, die Sie verwenden können: *Server* und *Workstation* Die Sortierungsregel funktioniert nur, wenn ein noch nicht in der Systemstruktur enthaltenes System den ePO-Server kontaktiert. Sie können für die Sortierungsregel einen Zeitplan aufstellen oder sie manuell ausführen.

Vorgehensweise

Gehen Sie wie nachfolgend beschrieben vor, um eine Sortierungsregel auf der Basis der Standard-Tags zu erstellen.

1 Wechseln Sie zu **Systeme |** Systemstruktur, und klicken Sie dann in der Menüleiste auf **Gruppe**.
2 Markieren Sie **Testgruppe**.
3 Suchen Sie oben auf der Seite **Gruppe** die Beschriftung **Sortierungskriterien**, und klicken Sie auf **Bearbeiten**.
4 Wählen Sie **Systeme, die mit einem der unten stehenden Sortierungskriterien übereinstimmen (IP-Adressen und/oder Tags)** aus. Es werden zusätzliche Optionen angezeigt.
5 Klicken Sie auf **Tag hinzufügen**.
6 Wählen Sie im Dropdownmenü den Eintrag **Server** aus, klicken Sie auf das Pluszeichen (**+**), und wählen Sie dann den Eintrag **Workstation** aus.
7 Klicken Sie auf **Speichern**.
8 Markieren Sie in der Systemstruktur **Eigene Organisation**.
9 Suchen Sie in der Liste **Sortierreihenfolge** den Eintrag für **Testgruppe.** Klicken Sie in der Spalte **Aktionen** auf **Nach oben**, bis die Gruppe an oberster Stelle der Liste angezeigt

wird. Diese Gruppe wird nun als erste bewertet, wenn neue Systeme in die Systemstruktur aufgenommen werden.

Weitere Informationen zum Arbeiten mit der Systemstruktur

Zur Organisation Ihrer Systemstruktur können Sie viele Typen von Gruppierungen verwenden.

Zusammen mit Gruppen können Sie Tags zu Ihren Systemen hinzufügen, um sie anhand der Systemeigenschaften weiter zu kennzeichnen.

Festlegen von Richtlinien für Endpunkte

Richtlinien werden verwendet, um die Konfiguration für die verschiedenen Total Protection for Endpoint-Produkte festzulegen, die auf Client-Systemen ausgeführt werden. Dazu gehören McAfee Agent und VirusScan Enterprise.

Damit Ihre Richtlinien die erforderlichen Konfigurationseinstellungen und Ausnahmen durchsetzen, empfiehlt McAfee das Erstellen der Richtlinien vor dem Durchführen von Richtlinienzuweisungen. Sie sollten den Namen einer Richtlinie so wählen, dass ihre Funktion deutlich wird. Wenn Sie auf diese Weise benannte Richtlinien erstellen, können diese einfacher anhand ihrer Rolle oder Funktion angewendet werden.

In diesem Abschnitt werden Sie durch einige Richtlinienänderungen für McAfee Agent, VirusScan Enterprise, Host Intrusion Prevention und SiteAdvisor Enterprise geführt, die in einer Produktionsumgebung hilfreich sein können. Die hier beschriebenen Schritte stellen die minimalen empfohlenen Richtlinienkonfigurationen dar. Sobald Sie die Suite fertig eingerichtet haben, können Sie weitere Richtlinienoptionen anpassen.

Wenn Sie alle Produkte in Total Protection for Endpoint installiert haben, empfiehlt McAfee, alle in diesem Abschnitt beschriebenen Schritte durchzuführen.

Erstellen von Richtlinien für McAfee Agent

Beim Testen von McAfee Total Protection for Endpoint ist es sinnvoll, die McAfee Agent-Richtlinie so zu ändern, dass das Taskleistensymbol auf Client-Systemen angezeigt wird. Auf diese Weise können Sie den Agenten-Statusmonitor anzeigen.

Ein anderer Grund für die Änderung der McAfee Agent-Richtlinie können langsame WAN-Verbindungen zu entfernten Niederlassungen oder eine große Zahl von verwalteten Knoten sein.

Sie können zum Beispiel festlegen, dass Systeme mit langsamen Verbindungen ePolicy Orchestrator aller 180 Minuten und damit 8 Mal täglich kontaktieren sollen. Die Standardeinstellung ist 24. In diesem Fall könnten Sie eine Richtlinie mit dem Namen "Niedrige Bandbreite" oder "3-Stunden-Abfrage" erstellen und die Option **Agent-zu-Server-Kommunikationsintervall** auf 180 Minuten statt der standardmäßigen 60 Minuten ändern.

Vorgehensweise

Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie zu erstellen, die McAfee Agent auf Client-Systemen anzeigt.

1. Wechseln Sie zu **Systeme | Richtlinienkatalog**.
2. Wählen Sie im Dropdownmenü **Produkt** den Eintrag **McAfee Agent** aus.
3. Klicken Sie in der Zeile mit dem Eintrag **McAfee Default** auf **Duplizieren**.
4. Geben Sie bei **Name** Agenten-Symbol anzeigen ein, und klicken Sie dann auf **OK**.
5. Klicken Sie in der Zeile mit der neuen Richtlinie auf **Bearbeiten**.
6. Aktivieren Sie das Kontrollkästchen neben **McAfee-Symbol in der Taskleiste anzeigen**, und klicken Sie auf **Speichern**.

ePolicy Orchestrator ermöglicht es Ihnen, remote auf das McAfee Agent-Protokoll jedes Systems zuzugreifen. Ausführliche Informationen zu diesem hilfreichen Tool zur Fehlerbehebung finden Sie im *ePolicy Orchestrator-Produkthandbuch*.

Erstellen von Richtlinien für VirusScan Enterprise

In diesem Abschnitt werden drei Beispiele von VirusScan Enterprise-Richtlinien behandelt. Die erste verhindert, dass Benutzer Einstellungen von VirusScan auf ihren verwalteten Systemen ändern. Die zweite legt Datenbankausschlüsse auf Servern fest. Die dritte ändert kurzzeitig die Richtlinie zu unerwünschten Programmen.

Sperren der lokalen VirusScan-Konsole

Gehen Sie wie nachfolgend beschrieben vor, um die standardmäßige VirusScan Enterprise-Benutzeroberflächenrichtlinie so zu ändern, dass Benutzer die lokale VirusScan-Benutzeroberfläche nicht verändern können. VirusScan Enterprise wird auf Workstations und Servern ausgeführt. Aus diesem Grund haben die VirusScan-Richtlinien getrennte Einstellungen für jede Plattform. In diesem Fall ändern Sie nur die Workstation-Einstellungen.

1. Wechseln Sie zu **Systeme |** Richtlinienkatalog.
2. Wählen Sie im Dropdownmenü **Produkt** den Eintrag **VirusScan Enterprise 8.7.0** aus.
3. Wählen Sie im Dropdownmenü **Kategorie** den Eintrag **Richtlinien für die Benutzeroberfläche** aus.
4. Klicken Sie in der Zeile mit dem Eintrag **McAfee Default** auf **Duplizieren**.
5. Geben Sie bei **Name** VSE-Konsole sperren ein, und klicken Sie dann auf **OK**.
6. Klicken Sie in der Zeile mit der neuen Richtlinie "VSE-Konsole sperren" auf **Bearbeiten**.
7. Klicken Sie in der Menüleiste auf **Kennwortoptionen**.
8. Vergewissern Sie sich, dass bei **Einstellungen für** der Eintrag **Workstation** ausgewählt ist.
9. Wählen Sie bei **Kennwort für Benutzerschnittstelle** die Option **Kennwortschutz für alle aufgelisteten Elemente** aus.
10. Geben Sie in die entsprechenden Felder ein Kennwort ein, und klicken Sie dann auf **Speichern**.

Erstellen von Dateiausschlüssen auf einem Server

Gehen Sie wie nachfolgend beschrieben vor, um eine VirusScan-Richtlinie zu erstellen, die zwei hypothetische Datenbankdateien auf einem Server ausschließt. Diese Art von Scan-Ausschlüssen ist typisch für viele Datenbank- und E-Mail-Server.

1. Wechseln Sie zu **Systeme |** Systemstruktur, und klicken Sie dann in der Menüleiste auf **Richtlinien**.
2. Wählen Sie im Dropdownmenü **Produkt** den Eintrag **VirusScan Enterprise 8.7.0** aus.
3. Erweitern Sie den Eintrag **Testgruppe**, und klicken Sie dann auf die Gruppe **Server**. Diese Richtlinie kann konfiguriert werden, bevor Sie Systeme zu dieser Gruppe hinzufügen.
4. Klicken Sie rechts neben **Richtlinien bei Zugriff für Standardvorgänge** auf **Zuweisung bearbeiten**.
5. Wählen Sie bei **Erben von** die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.
6. Klicken Sie bei **Zugewiesene Richtlinie** auf **Neue Richtlinie**.

7 Geben Sie im Dialogfeld **Neue Richtlinie erstellen** die Zeichenfolge Datenbank-AV-Ausschlüsse ein, und klicken Sie dann auf **OK**. Dadurch wird der Richtlinieneditor geöffnet.

8 Wählen Sie im Dropdownmenü **Einstellungen für** die Option **Server** aus.

9 Klicken Sie in der Menüleiste auf **Ausschlüsse**.

10 Klicken Sie bei **Elemente, die nicht gescannt werden sollen** auf **Hinzufügen**.

11 Wählen Sie im Dialogfeld den Eintrag **Nach Muster** aus, geben Sie data.mdf ein, und klicken Sie dann auf **OK**. Klicken Sie erneut auf **Hinzufügen**, geben Sie data.ldf als weiteren Ausschluss ein, und klicken Sie dann auf **OK**.

   In diesem Beispiel wird nur der Dateiname festgelegt. In einer Produktionsumgebung kann es notwendig sein, zum Eingrenzen Ihrer Ausschlüsse einen vollständigen Pfad festzulegen.

12 Wenn beide Ausschlüsse aufgeführt werden, klicken Sie auf **Speichern**.

13 Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** den Eintrag **Datenbank-AV-Ausschlüsse** aus, und klicken Sie dann auf **Speichern**.

Unter dem folgenden Link wird beschrieben, welche Ausschlüsse von Microsoft für Microsoft Exchange Server empfohlen werden, wenn unter Exchange 2007 Antivirenprüfungen auf Dateiebene durchgeführt werden sollen.

http://technet.microsoft.com/en-us/library/bb332342.aspx.

Eine VirusScan-Richtlinie wird für Microsoft Exchange Server-Umgebungen auf ähnliche Weise konfiguriert, enthält jedoch eine größere Anzahl von Ausschlüssen.

Erstellen von Richtlinien für das AntiSpyware Enterprise-Modul

Das AntiSpyware-Modul ist nach der Installation sofort aktiv und bereinigt oder löscht alle potenziell unerwünschten Programme (PUPs), die es entdeckt. Es erkennt und löscht Spyware und Adware. Möglicherweise sind auf Ihren Systemen andere PUPs installiert, die nicht entfernt werden sollen. Beispielsweise können in Ihrer IT-Abteilung Remote-Programme wie Verwaltungstools, Port-Scanner oder Kennwort-Cracker eingesetzt werden. Viele dieser Tools werden von Administratoren legal im Netzwerk verwendet.

In diesem Abschnitt wird beschrieben, wie Sie die vorhandenen PUPs in Ihrem Netzwerk finden, Ausschlüsse für legale PUPs erstellen und den Scanner so konfigurieren, dass alle anderen PUPs blockiert werden.

Hiermit werden die Einstellungen für den VirusScan-On-Access-Scan so geändert, dass entdeckte PUPs zwar protokolliert, jedoch nicht gelöscht werden. VirusScan erkennt und löscht weiterhin Viren, Würmer, Trojaner und andere potenziell unerwünschte Programme. Diese Vorgehensweise wird empfohlen, um die gemeldeten PUPs zunächst im "Audit-Modus" einige Tage oder Wochen lang zu überwachen, den PUP-Entdeckungsbericht in ePolicy Orchestrator zu überprüfen und die erforderlichen Ausschlüsse zu ermitteln.

Später können Sie die Richtlinienzuweisung so ändern, dass PUPs wieder bereinigt werden.

Vorgehensweise

Gehen Sie wie nachfolgend beschrieben vor, um die standardmäßige VirusScan-On-Access-Scan-Richtlinie so zu ändern, dass PUPs auf den verwalteten Systemen überwacht werden.

1 Wechseln Sie zu **Systeme |** Richtlinienkatalog.

2 Wählen Sie im Dropdownmenü **Produkt** den Eintrag **VirusScan Enterprise 8.7.0** aus.

3 Wählen Sie in der Spalte **Kategorie** die Option **Richtlinien bei Zugriff für Standardvorgänge** aus.

4 Klicken Sie in der Zeile mit dem Eintrag **McAfee Default** auf **Duplizieren**.
5 Geben Sie bei **Name** Audit für PUPs ein, und klicken Sie dann auf **OK**.
6 Klicken Sie in der Zeile mit der neuen Richtlinie auf **Bearbeiten**.
7 Wählen Sie im Dropdownmenü **Einstellungen für** die Option **Workstation** aus.
8 Klicken Sie in der Menüleiste auf **Aktionen**.
9 Wählen Sie für **Wenn ein unerwünschtes Programm gefunden wird** im Dropdownmenü als erste durchzuführende Aktion **Zugriff auf Dateien erlauben** aus. Dadurch wird die sekundäre Aktion deaktiviert.
10 Klicken Sie auf **Speichern**.

Erstellen von Richtlinien für SiteAdvisor Enterprise Plus

In diesem Abschnitt wird beschrieben, wie Sie eine Richtlinie für Bewertungsaktionen und Erzwingungsmitteilungen für SiteAdvisor Enterprise Plus erstellen.

Erstellen einer Richtlinie für Bewertungsaktionen

Gehen Sie wie nachfolgend beschrieben vor, um eine neue Richtlinie zu erstellen, die Benutzer daran hindert, Webseiten mit Bedrohungen aufzurufen oder sie vor potenziellen Bedrohungen auf Webseiten warnt.

Mit den Optionen für die Richtlinien für Bewertungsaktionen können Sie die SiteAdvisor-Einstufungen (grün, gelb, rot oder nicht bewertet) verwenden, um festzulegen, ob Benutzer auf eine Webseite oder deren Ressource (z. B. Download-Dateien) zugreifen können.

- Legen Sie für jede gelbe, rote oder nicht bewertete Webseite fest, ob sie zulässig ist, eine Warnung generiert werden oder die Webseite blockiert werden soll.
- Legen Sie für jede gelbe, rote oder nicht bewertete Download-Datei fest, ob sie zulässig ist, eine Warnung generiert werden oder der Download blockiert werden soll. Auf diese Weise kann genauer festgelegt werden, wie Benutzer vor einzelnen Dateien geschützt werden sollen, die auf Webseiten mit insgesamt grüner Bewertung eine Bedrohung darstellen können.
- Legen Sie bei allen Phishing-Webseiten fest, ob der Zugriff blockiert oder gewährt werden soll. Auf diese Weise kann genauer festgelegt werden, wie Benutzer vor einzelnen Seiten mit Phishing-Techniken geschützt werden sollen, die auf Webseiten mit insgesamt grüner Bewertung eine Bedrohung darstellen können.

Vorgehensweise

1 Wechseln Sie zu **Systeme | **Richtlinienkatalog.
2 Wählen Sie im Dropdownmenü **Produkt** den Eintrag **SiteAdvisor Enterprise Plus** aus.
3 Wählen Sie im Dropdownmenü **Kategorie** den Eintrag **Richtlinie für Bewertungsaktionen** aus.
4 Klicken Sie in der Zeile mit dem Eintrag **McAfee Default** auf **Duplizieren**.
5 Geben Sie bei **Name** Richtlinie für Bewertungsaktionen ein, und klicken Sie dann auf **OK**.
6 Klicken Sie in der Zeile mit der neuen Richtlinie auf **Bearbeiten**.
7 Legen Sie bei **Aktionen zur Site-Navigationsbewertung** die Optionen **Warnen** für gelbe Sites, **Blockieren** für rote Sites und **Warnen** für nicht bewertete Sites fest.
8 Klicken Sie auf **Speichern**.

Erstellen einer Richtlinie für Erzwingungsmitteilungen

Gehen Sie wie nachfolgend beschrieben vor, um eine neue Richtlinie zum Anpassen von Nachrichten zu erstellen, die Benutzern beim Aufrufen von Webseiten angezeigt werden, deren

Bewertung Sie mit einer Aktion verknüpft haben. Diese Nachricht wird in Infosymbolen oder auf Warnungs- oder Blockierungs-Seiten angezeigt.

Vorgehensweise

1. Wechseln Sie zu **Systeme | Richtlinienkatalog**.
2. Wählen Sie im Dropdownmenü **Produkt** den Eintrag **SiteAdvisor Enterprise Plus** aus.
3. Wählen Sie im Dropdownmenü **Kategorie** den Eintrag **Richtlinie für Erzwingungsmitteilungen** aus.
4. Klicken Sie in der Zeile mit dem Eintrag **McAfee Default** auf **Duplizieren**.
5. Geben Sie bei **Name** Richtlinie für Erzwingungsmitteilungen ein, und klicken Sie dann auf **OK**.
6. Klicken Sie in der Zeile mit der neuen Richtlinie auf **Bearbeiten**.
7. Klicken Sie auf die Registerkarte **Site**.
8. Wählen Sie eine Sprache aus.
9. Geben Sie eine Nachricht mit maximal 50 Zeichen für folgende Fälle ein:
   - Bei Sites, für die Sie **Warnen** festgelegt haben, geben Sie eine Warnmeldung ein.
   - Bei Sites, für die Sie **Blockieren** festgelegt haben, geben Sie eine Nachricht über blockierten Zugriff ein.
   - Bei Sites, für die Sie **Zulassen** festgelegt haben, geben Sie eine Nachricht über gewährten Zugriff ein.
10. Klicken Sie auf **Speichern**.

Zuweisen von Richtlinien zu Systemen

Sie verfügen jetzt über mehrere Richtlinien, die Sie den Systemen in der Systemstruktur zuweisen können. In dieser Anleitung weisen Sie alle Richtlinien mithilfe der Systemstruktur-Schnittstelle zu.

1. Wechseln Sie zu **Systeme | Systemstruktur**, und klicken Sie dann in der Menüleiste auf **Richtlinien**.
2. Markieren Sie **Testgruppe**.
3. Weisen Sie die McAfee Agent-Richtlinie zu:
   - Wählen Sie im Dropdownmenü **Produkt** den Eintrag **McAfee Agent** aus.
   - Klicken Sie in der Zeile mit dem Eintrag **My Default** auf **Zuweisung bearbeiten**.
   - Wählen Sie bei **Erben von** die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.
   - Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** den Eintrag **Agenten-Symbol anzeigen** aus.
   - Klicken Sie auf **Speichern**.
4. Weisen Sie die SiteAdvisor Enterprise Plus-Richtlinien zu:
   - Wählen Sie im Dropdownmenü **Produkt** den Eintrag **SiteAdvisor Enterprise Plus** aus.
   - Klicken Sie in der Zeile mit dem Eintrag **Bewertungsaktionen** auf **Zuweisung bearbeiten**.
   - Wählen Sie bei **Erben von** die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.

- Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** den Eintrag **Richtlinie für Bewertungsaktionen** aus.
- Klicken Sie auf **Speichern**.
- Klicken Sie in der Zeile mit dem Eintrag **Erzwingungsmitteilungen** auf **Zuweisung bearbeiten**.
- Wählen Sie bei **Erben von** die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.
- Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** den Eintrag **Richtlinie für Erzwingungsmitteilungen** aus.
- Klicken Sie auf **Speichern**.

5 Weisen Sie die VirusScan Enterprise-Richtlinien zu:

HINWEIS: Als Sie die Richtlinie "Datenbank-AV-Ausschlüsse" erstellt haben, haben Sie diese der Gruppe "Server" zugewiesen.

- Wählen Sie im Dropdownmenü **Produkt** den Eintrag **VirusScan Enterprise 8.7.0** aus.
- Klicken Sie in der Zeile mit dem Eintrag **Richtlinien für die Benutzeroberfläche** auf **Zuweisung bearbeiten**.
- Wählen Sie bei **Erben von** die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.
- Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** den Eintrag **VSE-Konsole sperren** aus.
- Klicken Sie auf **Speichern**.
- Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** den Eintrag **Richtlinien bei Zugriff für Standardvorgänge** aus, und wählen Sie dann **Audit für PUPs**.
- Klicken Sie auf **Speichern**. Wenn Sie die Seite **Richtlinien** wieder aufrufen, sehen Sie, dass die Spalte **Vererbung unterbrochen** einen Eintrag für **Richtlinien bei Zugriff für Standardvorgänge** enthält. Der Grund dafür ist, dass Sie die Richtlinie "Datenbank-AV-Ausschlüsse" bereits der Gruppe "Server" zugewiesen haben.

Host Intrusion Prevention-Richtlinien

McAfee Host Intrusion Prevention bietet drei Arten von Schutz: IPS, Firewall und Anwendungssperre. Bei einer Standardinstallation ist der IPS-Schutz auf die Verhinderung von Eindringungen mit hohem Schweregrad festgelegt, und die Firewall und die Richtlinien zum Blockieren von Anwendungen sind deaktiviert. Auf diese Weise wird gleich nach der Installation der grundlegende Schutz von VirusScan Enterprise vor Buffer Overflows erweitert, wobei gleichzeitig Schutz vor vielen Microsoft-Schwachstellen besteht – ohne die geschäftlichen Abläufe zu beeinträchtigen.

In diesem Abschnitt wird beschrieben, wie Sie eine grundlegende Firewall-Richtlinie erstellen. Außerdem erhalten Sie Hinweise zu anderen Regeln, die Sie möglicherweise anwenden oder anpassen möchten. Firewall-Regelrichtlinien enthalten Regeln zum Zulassen und Blockieren des Datenverkehrs auf den geschützten Rechnern. Mit McAfee können Sie auf einfache Weise mithilfe von vorkonfigurierten Richtlinien in Host Intrusion Prevention einen Endpunkt-Firewall-Schutz einrichten.

Die Richtlinie für die typische Unternehmensumgebung kann als grundlegende Firewall-Richtlinie verwendet werden. Diese Richtlinie enthält alle Funktionen, die in den meisten Unternehmen benötigt werden. Verwenden Sie diese Richtlinie als Ausgangspunkt, und nutzen Sie die

Ergebnisse des adaptiven Modus, um zusätzliche Regeln anzuwenden und zu überprüfen. Diese Richtlinie sollte – im Vergleich zu vorhandenen standardmäßigen Firewall-Richtlinien – weniger gelernte Client-Regeln im adaptiven Modus generieren.

Wenn Sie zum ersten Mal eine Firewall-Richtlinie ausbringen, kann es sinnvoll sein, dass die Clients die unterschiedlichen Kommunikationsanforderungen der jeweiligen Anwendungen auf den geschützten Computern lernen. Dieser Lernprozess wird als *adaptiver Modus* bezeichnet. In diesem Modus fügt die Firewall der Richtlinie automatisch die Regeln hinzu, die den Datenverkehr zulassen, der noch nicht von der Firewall-Regelrichtlinie abgedeckt wird. Dazu ist keine Bestätigung der Benutzer erforderlich. Bei jeder Agent-Server-Kommunikation sendet McAfee Agent alle auf dem Client-Computer neu gelernten Regeln an ePolicy Orchestrator. Sie können diese "auf dem Client gelernten Regeln" auf der Benutzeroberfläche unter **Berichterstellung |** Host IPS überprüfen. Auf diesem Bildschirm wird angezeigt, welche Regeln von den Host Intrusion Prevention-Clients hinzugefügt wurden, und diese Regeln zu den Richtlinien hinzufügen.

Detaillierte Hinweise zum Anpassen von nicht standardmäßigen IPS-Funktionen finden Sie im Whitepaper *Adopting McAfee Host Intrusion Prevention: Best practices for quick success* (Einsatz von McAfee Host IPS: Der einfachste Weg zum Erfolg), das Sie vom McAfee-Support oder den McAfee-Vertriebsmitarbeitern erhalten.

Gehen Sie wie nachfolgend beschrieben vor, um Firewall-Regeln auf Grundlage der Vorlage für typische Unternehmensumgebungen festzulegen und für die Firewall-Optionen den adaptiven Modus zu aktivieren.

Zuweisen einer Firewall-Regelrichtlinie

1 Wechseln Sie zu **Systeme |** Systemstruktur, und wählen Sie dann in der Menüleiste **Richtlinien** aus.
2 Erweitern Sie in der **Systemstruktur** den Eintrag **Testgruppe**, und markieren Sie dann die Gruppe **Workstations**.
3 Wählen Sie im Dropdownmenü **Produkt** den Eintrag **Host Intrusion Prevention 7.X.X:Firewall** aus.
4 Suchen Sie in der Spalte **Kategorie** den Eintrag **Firewall-Regeln (Windows)**, und klicken Sie dann auf **Zuweisung bearbeiten**.
5 Wählen Sie bei **Erben von** die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.
6 Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** den Eintrag **Typische Unternehmensumgebung** aus.
7 Klicken Sie auf **Richtlinie bearbeiten**, und überprüfen Sie die vorhandenen Regeleinstellungen.
8 Klicken Sie auf **Abbrechen**, um die Seite **Richtlinie bearbeiten** zu schließen.
9 Klicken Sie auf der Seite **Richtliniezuweisung** auf **Speichern**.

Wenn Sie die Regeleinstellungen der Richtlinie **Typische Unternehmensumgebung** ändern möchten, können Sie diese duplizieren und an der Richtlinienkopie die gewünschten Änderungen vornehmen.

Festlegen der Firewall-Optionen

1 Wechseln Sie zu **Systeme |** Systemstruktur, und wählen Sie dann in der Menüleiste **Richtlinien** aus.
2 Erweitern Sie in der **Systemstruktur** den Eintrag **Testgruppe**, und markieren Sie dann die Gruppe **Workstations**.

3 Wählen Sie im Dropdownmenü **Produkt** den Eintrag **Host Intrusion Prevention 7.X.X:Firewall** aus.

4 Suchen Sie in der Spalte **Kategorie** den Eintrag **Firewall-Optionen (Windows)**, und klicken Sie dann auf **Zuweisung bearbeiten**.

5 Wählen Sie bei **Erben von** die Option **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.

6 Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** den Eintrag **Adaptiv** aus. Damit werden für Datenverkehr, der von der Firewall-Regelrichtlinie noch nicht abgedeckt wird, Regeln erstellt.

7 Klicken Sie auf **Speichern**.

Weitere Informationen zum Verwalten der Host Intrusion Prevention-Firewall finden Sie im *Host Intrusion Prevention Product Guide* (Host Intrusion Prevention – Produkthandbuch). Im Abschnitt "Verweise" finden Sie Links zu technischen Kurzinformationen und zu anderen Dokumentationen.

Einstellen von Richtlinien für E-Mail-Server

McAfee GroupShield bietet Schutz für Ihre Microsoft Exchange- und Lotus Domino-Server. Es schützt vor Viren, unerwünschtem Inhalt, potenziell unerwünschten Programmen, gesperrten Dateitypen/Nachrichten und unterstützt die Inhaltsfilterung in E-Mail-Nachrichten.

Über ein Zusatzpaket unterstützt GroupShield außerdem Anti-Spam- und Anti-Phishing-Funktionen für eingehende Nachrichten. Zusätzlich gleicht es jede E-Mail-Nachricht mit einem umfangreichen Satz von Regeln ab und berechnet dann eine Spam-Gesamtbewertung.

GroupShield for Exchange-Richtlinien

In den folgenden Abschnitten erstellen Sie GroupShield for Microsoft Exchange-Beispielrichtlinien für den gesperrten Inhalt, Anti-Spam- und Anti-Phishing-Scanner. McAfee empfiehlt die Verwendung der standardmäßig festgelegten Antiviren-Richtlinien. Beginnen Sie mit den standardmäßigen Anti-Spam-Richtlinien, und nehmen Sie je nach Bedarf eine Feineinstellung der Schwellenwerte vor. Die Beispiele dienen nur zur Veranschaulichung.

Konfigurieren von Richtlinien für gesperrte Inhalte

In diesem Abschnitt finden Sie ein Beispiel zum Filtern gesperrter Inhalte. Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie zu erstellen, nach der bei jeder E-Mail mit Dokumentanhang, der die Worte "Vertrauliche Informationen" enthält, die Nachricht durch einem Alarm ersetzt und eine Benachrichtigung an den Administrator gesendet werden soll.

1. Wechseln Sie zu **Systeme | Richtlinienkatalog**.
2. Wählen Sie im Dropdownmenü **Produkt** den Eintrag **GroupShield for Exchange 7.0.0** aus.
3. Wählen Sie im Dropdownmenü **Kategorie** den Eintrag **Scannereinstellungen** aus.
4. Klicken Sie in der Zeile mit dem Eintrag **My Default** auf **Duplizieren**.
5. Geben Sie bei **Name** Eigene Exchange-Richtlinie ein, und klicken Sie dann auf **OK**.
6. Klicken Sie in der Zeile mit dem Eintrag **Eigene Exchange-Richtlinie** auf **Bearbeiten**.
7. Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**.
8. Klicken Sie auf die Registerkarte **Filterregeln**.
9. Klicken Sie zum Erstellen einer neuen Kategorie von Regeln für Inhaltsscanner auf **Neue Kategorie**.
10. Geben Sie bei **Name** Inhalt ein, und klicken Sie dann auf **OK**.
11. Klicken Sie zum Erstellen einer neuen Regel für die Kategorie unter **Regeln für Inhaltsscanner** auf **Neue erstellen**.
12. Geben Sie für **Regelname** Blockierter Inhalt ein.
13. Geben Sie eine Beschreibung ein, und aktivieren Sie die Option **Diese Regel zur Regelgruppe dieser Kategorie hinzufügen**.

14 Wählen Sie die Registerkarte **Wort oder Ausdruck** aus. Geben Sie in das Feld **Die Regel wird ausgelöst, wenn das folgende Wort oder der folgende Ausdruck gefunden wird** Vertrauliche Informationen ein.

15 Wählen Sie die Registerkarte **Dateiformat** aus. Deaktivieren Sie die Option **Alles**. Wählen Sie unter **Dateikategorien** den Eintrag **Dokumente** aus. Wählen Sie unter **Unterkategorien** den Eintrag **Alle** aus.

16 Klicken Sie auf **Speichern**.

17 Klicken Sie auf der Seite **Gemeinsam benutzte Ressource** noch einmal auf **Speichern**.

18 Klicken Sie unter **Richtlinien-Manager** auf **Bei Zugriff**.

19 Klicken Sie auf **Masterrichtlinie**.

20 Wählen Sie unter **Haupt-Scanner** für **Inhaltsscan** den Wert **Aktiv** aus. Klicken Sie in der Spalte **Name** auf **Inhaltsscan**.

21 Wählen Sie die Registerkarte **Einstellungen anzeigen** aus. Wählen Sie im Dropdownmenü **Auswahl** den Eintrag **Inhaltsscan** aus.

22 Aktivieren Sie unter **Optionen** die Punkte **Dokument- und Datenbankformate in Inhaltsscan einschließen** und **Alle Anlagen scannen**.

23 Wenn die Warnung angezeigt wird, dass dies eine höhere CPU-Auslastung verursacht, klicken Sie auf **OK**.

24 Klicken Sie im Abschnitt **Regeln und zugeordnete Aktionen für Inhaltsscanner** auf **Regel hinzufügen**.

25 Wählen Sie im Dropdownmenü **Regelgruppe auswählen** den Eintrag **Inhalt** aus. Die Option **Regeln aus dieser Gruppe auswählen** sollte den Eintrag "Blockierter Inhalt" enthalten.

26 Wählen Sie im Dropdownmenü **Bei Entdeckung die folgende Aktion durchführen** den Eintrag **Element durch Warnung ersetzen** aus. Wählen Sie im Abschnitt **Und außerdem** den Eintrag **Administrator benachrichtigen** aus.

27 Klicken Sie auf **Speichern**.

28 Klicken Sie auf der Seite **Bei Zugriff** noch einmal auf **Speichern**.

Konfigurieren von Richtlinien für Anti-Spam-Scanner

Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie zu konfigurieren, nach der jede Spam-E-Mail mit einem hohen Faktor abgewiesen wird.

1 Wechseln Sie zu **Systeme |** Richtlinienkatalog.

2 Wählen Sie im Dropdownmenü **Produkt** den Eintrag **GroupShield for Exchange 7.0.0** aus.

3 Wählen Sie im Dropdownmenü **Kategorie** den Eintrag **Scannereinstellungen** aus.

4 Klicken Sie in der Zeile mit dem Eintrag **Eigene Exchange-Richtlinie** auf **Bearbeiten**.

5 Klicken Sie unter **Richtlinien-Manager** auf **Gateway**.

6 Klicken Sie auf **Masterrichtlinie**.

7 Klicken Sie auf die Registerkarte **Einstellungen anzeigen**. Wählen Sie im Dropdownmenü **Auswahl** den Eintrag **Anti-Spam** aus.

8 Klicken Sie im Abschnitt **Durchzuführende Aktionen bei Erkennung von Spam** auf **Bearbeiten**.

9 Klicken Sie auf die Registerkarte **Hoher Faktor**.

10 Wählen Sie im Dropdownmenü **Die folgende Aktion durchführen** den Eintrag **Nachricht ablehnen** aus. Wählen Sie im Abschnitt **Und außerdem** den Eintrag **Nachricht isolieren** aus.
11 Klicken Sie auf **Speichern**.
12 Klicken Sie auf der Seite **Gateway** noch einmal auf **Speichern**.

Konfigurieren von Richtlinien für Anti-Phishing-Scanner

Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie zu konfigurieren, die jede Phishing-E-Mail protokolliert.

1 Wechseln Sie zu **Systeme | ** Richtlinienkatalog.
2 Wählen Sie im Dropdownmenü **Produkt** den Eintrag **GroupShield for Exchange 7.0.0** aus.
3 Wählen Sie im Dropdownmenü **Kategorie** den Eintrag **Scannereinstellungen** aus.
4 Klicken Sie in der Zeile mit dem Eintrag **Eigene Exchange-Richtlinie** auf **Bearbeiten**.
5 Klicken Sie unter **Richtlinien-Manager** auf **Gateway**.
6 Klicken Sie auf **Masterrichtlinie**, oder, wenn Sie sich noch auf der Seite **Eigene Exchange-Richtlinie** befinden, wählen Sie im Dropdownmenü **Richtlinie** den Eintrag **Masterrichtlinie** aus.
7 Klicken Sie auf die Registerkarte **Einstellungen anzeigen**. Wählen Sie im Dropdownmenü **Auswahl** den Eintrag **Anti-Phishing** aus.
8 Klicken Sie im Bereich **Aktionen** auf **Bearbeiten**.
9 Wählen Sie im Abschnitt **Und außerdem** den Eintrag **Protokollieren** aus.
10 Klicken Sie auf **Speichern**.
11 Klicken Sie auf der Seite **Gateway** noch einmal auf **Speichern**.

Zuweisen von Richtlinien zu Exchange-Servern

Gehen Sie wie nachfolgend beschrieben vor, um die konfigurierten Richtlinien zu Ihren Microsoft Exchange-Servern zuzuweisen.

1 Wechseln Sie zu **Systeme | ** Systemstruktur, und klicken Sie dann in der Menüleiste auf **Richtlinien**.
2 Erweitern Sie die Option **Testgruppe**, und markieren Sie **Server**.
3 Wählen Sie im Dropdownmenü **Produkt** den Eintrag **GroupShield for Exchange 7.0.0** aus.
4 Klicken Sie in der Zeile mit den Scannereinstellungen auf **Zuweisung bearbeiten**.
5 Wählen Sie **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.
6 Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** den Eintrag **Eigene Exchange-Richtlinie** aus.
7 Klicken Sie auf **Speichern**.
8 Klicken Sie in der Menüleiste auf **Systeme**.
9 Klicken Sie auf **Weitere Aktionen**, und wählen Sie **Agenten reaktivieren** aus.
10 Legen Sie unter **McAfee Agent reaktivieren** für die Option **Zufallsgenerator** null Minuten fest.
11 Klicken Sie auf **OK**.

GroupShield for Domino-Richtlinien

In den folgenden Abschnitten erstellen Sie GroupShield für IBM Lotus Domino-Beispielrichtlinien für den gesperrten Inhalt, Anti-Spam- und Anti-Phishing-Scanner. McAfee empfiehlt die Verwendung der standardmäßig festgelegten Antiviren-Richtlinien. Beginnen Sie mit den standardmäßigen Anti-Spam-Richtlinien, und nehmen Sie je nach Bedarf eine Feineinstellung der Schwellenwerte vor. Die Beispiele dienen nur zur Veranschaulichung.

Konfigurieren von Richtlinien für gesperrte Inhalte

In diesem Abschnitt finden Sie ein Beispiel zum Filtern gesperrter Inhalte. Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie zu erstellen, nach der bei jeder E-Mail mit Dokumentanhang, der die Worte "Vertrauliche Informationen" enthält, die Nachricht durch einem Alarm ersetzt und eine Benachrichtigung an den Administrator gesendet werden soll.

1. Wechseln Sie zu **Systeme | Richtlinienkatalog**.
2. Wählen Sie im Dropdownmenü **Produkt** den Eintrag **GroupShield for Lotus Domino 7.0.0** aus.
3. Wählen Sie im Dropdownmenü **Kategorie** den Eintrag **Scannereinstellungen** aus.
4. Klicken Sie in der Zeile mit dem Eintrag **My Default** auf **Duplizieren**.
5. Geben Sie bei **Name** Eigene Domino-Richtlinie ein, und klicken Sie dann auf **OK**.
6. Klicken Sie in der Zeile mit dem Eintrag **Eigene Domino-Richtlinie** auf **Bearbeiten**.
7. Klicken Sie unter **Richtlinien-Manager** auf **Gemeinsam benutzte Ressource**.
8. Klicken Sie auf die Registerkarte **Filterregeln**.
9. Klicken Sie zum Erstellen einer neuen Kategorie von Regeln für Inhaltsscanner auf **Neue Kategorie**.
10. Geben Sie bei **Name** Inhalt ein, und klicken Sie dann auf **OK**.
11. Klicken Sie zum Erstellen einer neuen Regel für die Kategorie unter **Regeln für Inhaltsscanner** auf **Neue erstellen**.
12. Geben Sie für **Regelname** Blockierter Inhalt ein.
13. Geben Sie eine Beschreibung ein, und aktivieren Sie die Option **Diese Regel zur Regelgruppe dieser Kategorie hinzufügen**.
14. Wählen Sie die Registerkarte **Wort oder Ausdruck** aus. Geben Sie in das Feld **Die Regel wird ausgelöst, wenn das folgende Wort oder der folgende Ausdruck gefunden wird** Vertrauliche Informationen ein.
15. Wählen Sie die Registerkarte **Dateiformat** aus. Deaktivieren Sie die Option **Alles**. Wählen Sie unter **Dateikategorien** den Eintrag **Dokumente** aus. Wählen Sie unter **Unterkategorien** den Eintrag **Alle** aus.
16. Klicken Sie auf **Speichern**.
17. Klicken Sie auf der Seite **Gemeinsam benutzte Ressource** noch einmal auf **Speichern**.
18. Klicken Sie unter **Richtlinien-Manager** auf **Externe Nachrichten**.
19. Klicken Sie auf **Masterrichtlinie**.
20. Aktivieren Sie unter **Kernscanner** für **Inhaltsscan** das Kontrollkästchen **Aktiv**. Klicken Sie in der Spalte **Name** auf **Inhaltsscan**.
21. Wählen Sie die Registerkarte **Einstellungen anzeigen** aus. Wählen Sie im Dropdownmenü **Auswahl** den Eintrag **Inhaltsscan** aus.
22. Aktivieren Sie unter **Optionen** die Punkte **Dokument- und Datenbankformate in Inhaltsscan einbeziehen** und **Text aller Anlagen scannen**.

23 Wenn die Warnung angezeigt wird, dass dies eine höhere CPU-Auslastung verursacht, klicken Sie auf **OK.**

24 Klicken Sie im Abschnitt **Regeln und zugeordnete Aktionen für Inhaltsscanner** auf **Regel hinzufügen**.

25 Wählen Sie im Dropdownmenü **Regelgruppe auswählen** den Eintrag **Inhalt** aus. Die Option **Regeln aus dieser Gruppe auswählen** sollte den Eintrag "Blockierter Inhalt" enthalten.

26 Wählen Sie im Dropdownmenü **Bei Erkennung die folgende Aktion durchführen** den Eintrag **Element durch Warnung ersetzen** aus. Wählen Sie im Abschnitt **Und ebenfalls** den Eintrag **Administrator benachrichtigen** aus.

27 Klicken Sie auf **Speichern**.

28 Klicken Sie auf der Seite **Externe E-Mails** noch einmal auf **Speichern**.

Konfigurieren von Richtlinien für Anti-Spam-Scanner

Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie zu konfigurieren, nach der jede Spam-E-Mail mit einem hohen Faktor abgewiesen wird.

1 Wechseln Sie zu **Systeme |** Richtlinienkatalog.

2 Wählen Sie im Dropdownmenü **Produkt** den Eintrag **GroupShield for Lotus Domino 7.0.0** aus.

3 Wählen Sie im Dropdownmenü **Kategorie** den Eintrag **Scannereinstellungen** aus.

4 Klicken Sie in der Zeile mit dem Eintrag **Eigene Domino-Richtlinie** auf **Bearbeiten**.

5 Klicken Sie unter **Richtlinien-Manager** auf **Externe Nachrichten**.

6 Klicken Sie auf **Masterrichtlinie**.

7 Klicken Sie auf die Registerkarte **Einstellungen anzeigen**. Wählen Sie im Dropdownmenü **Auswahl** den Eintrag **Anti-Spam** aus.

8 Klicken Sie im Abschnitt **Durchzuführende Aktionen bei Erkennung von Spam** auf **Bearbeiten**.

9 Klicken Sie auf die Registerkarte **Hoher Faktor**.

10 Wählen Sie im Dropdownmenü **Die folgende Aktion durchführen** den Eintrag **Nachricht ablehnen** aus. Wählen Sie im Abschnitt **Und ebenfalls** den Eintrag **Nachricht isolieren** aus.

11 Klicken Sie auf **Speichern**.

12 Klicken Sie auf der Seite **Externe E-Mails** noch einmal auf **Speichern**.

Konfigurieren von Richtlinien für Anti-Phishing-Scanner

Gehen Sie wie nachfolgend beschrieben vor, um eine Richtlinie zu konfigurieren, die jede Phishing-E-Mail protokolliert.

1 Wechseln Sie zu **Systeme |** Richtlinienkatalog.

2 Wählen Sie im Dropdownmenü **Produkt** den Eintrag **GroupShield for Lotus Domino 7.0.0** aus.

3 Wählen Sie im Dropdownmenü **Kategorie** den Eintrag **Scannereinstellungen** aus.

4 Klicken Sie in der Zeile mit dem Eintrag **Eigene Domino-Richtlinie** auf **Bearbeiten**.

5 Klicken Sie unter **Richtlinien-Manager** auf **Externe Nachrichten**.

6 Klicken Sie auf **Masterrichtlinie**, oder, wenn Sie sich noch auf der Seite **Eigene Domino-Richtlinie** befinden, wählen Sie im Dropdownmenü **Richtlinie** den Eintrag **Masterrichtlinie** aus.

7 Klicken Sie auf die Registerkarte **Einstellungen anzeigen**. Wählen Sie im Dropdownmenü **Auswahl** den Eintrag **Anti-Phishing** aus.

8 Klicken Sie im Bereich **Aktionen** auf **Bearbeiten**.

9 Wählen Sie im Abschnitt **Und ebenfalls** den Eintrag **Protokollieren** aus.

10 Klicken Sie auf **Speichern**.

11 Klicken Sie auf der Seite **Gateway** noch einmal auf **Speichern**.

Zuweisen von Richtlinien zu IBM Lotus Domino-Servern

Gehen Sie wie nachfolgend beschrieben vor, um die konfigurierten Richtlinien zu Ihren IBM Lotus Domino-Servern zuzuweisen.

1 Wechseln Sie zu **Systeme | ** Systemstruktur, und klicken Sie dann in der Menüleiste auf **Richtlinien**.

2 Erweitern Sie die Option **Testgruppe**, und markieren Sie **Server**.

3 Wählen Sie im Dropdownmenü **Produkt** den Eintrag **GroupShield for Lotus Domino 7.0.0** aus.

4 Klicken Sie in der Zeile mit den Scannereinstellungen auf **Zuweisung bearbeiten**.

5 Wählen Sie **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.

6 Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** den Eintrag **Eigene Domino-Richtlinie** aus.

7 Klicken Sie auf **Speichern**.

8 Klicken Sie in der Menüleiste auf **Systeme**.

9 Klicken Sie auf **Weitere Aktionen**, und wählen Sie **Agenten reaktivieren** aus.

10 Legen Sie unter **McAfee Agent reaktivieren** für die Option **Zufallsgenerator** null Minuten fest.

11 Klicken Sie auf **OK**.

Festlegen von Endpunkt-Tasks

Sie haben nun eine Systemstruktur erstellt, Client-Systeme hinzugefügt, die Software eingecheckt und Ihre Richtlinien konfiguriert. Als nächstes planen Sie die Ausbringung von VirusScan Enterprise und der anderen Sicherheitsprodukte. Die Produktausbringung erfolgt mithilfe eines Client-Tasks, den McAfee Agent abruft und ausführt. Sie können Client-Tasks auch zum Planen von Scans und zum Aktualisieren verwenden.

Nachdem Sie die Ausbringungs- und Aktualisierungs-Tasks in diesem Abschnitt erstellt haben, erstellen Sie einen VirusScan Enterprise-Task "On-Demand-Scan". Klicken Sie auf den Link und führen Sie die Schritte aus der Online-Hilfe aus.

Erstellen eines Ausbringungs-Tasks

In diesem Abschnitt erstellen Sie einen Client-Task, der ein oder mehrere Produkte auf eine Gruppe von Systemen ausbringt. Dabei wird davon ausgegangen, dass Sie alle Endpunkt-Produkte während der Installation eingecheckt haben. Andernfalls sind nur die eingecheckten Produkte in der Produktliste verfügbar (Schritt 5).

1. Wechseln Sie zu **Systeme | Systemstruktur**, und klicken Sie dann in der Menüleiste auf **Client-Tasks**.
2. Markieren Sie **Eigene Organisation**, und klicken Sie dann auf **Neuer Task**.
3. Geben Sie als Namen McAfee-Ausbringung ein.
4. Wählen Sie im Dropdownmenü **Typ** den Eintrag **Produktausbringung (McAfee Agent)** aus, und klicken Sie anschließend auf **Weiter**.
5. Wählen Sie auf der Seite **Konfiguration** unter **Produkte und Komponenten** Ihre Endpunkt-Produkte aus. Mit dem Pluszeichen (**+**) können Sie weitere Zeilen hinzufügen. Wählen Sie unter **Aktion** für jedes Produkt **Installieren** aus, und legen für **Sprache** die auf Ihren Client-Systemen verwendete Sprache fest. Gehen Sie in der Dropdownliste **Produkt** folgendermaßen vor:
   - Wählen Sie **VirusScan Enterprise 8.7.0.xxx** aus, und klicken Sie dann auf **+**.
   - Wählen Sie **AntiSpyware Enterprise Module 8.7.0.xxx** aus, und klicken Sie dann auf **+**.
   - Wählen Sie **Host Intrusion Prevention 7.0.0.xxx** aus, und klicken Sie dann auf **+**.
   - Wählen Sie **SiteAdvisor Enterprise Plus 2.0.0.xxx** aus.
6. Wählen Sie **Bei jeder Richtlinienumsetzung ausführen** aus, und klicken Sie dann auf **Weiter**.
7. Wählen Sie auf der Seite **Plan** die folgenden Optionen aus, und klicken Sie dann auf **Weiter**:

Planungsstatus	**Aktiviert**
Planungstyp	**Sofort ausführen**

8. Klicken Sie auf der Seite **Zusammenfassung** auf **Speichern**.

Beim Ausbringen einer großen Anzahl an Systemen in einer Produktionsumgebung empfiehlt McAfee, die Option **Zufallsgenerator** auf der Seite **Plan** zu verwenden. Mithilfe des

Zufallsgenerators können Sie vermeiden, dass die Client-Systeme zu viele Anforderungen gleichzeitig an den Server senden. Wahrscheinlich möchten Sie in einer realen Umgebung Ausbringungen für bestimmte Tageszeiten planen. Wenn der Plan auf **Sofort ausführen** eingestellt ist, wird die Ausbringung für Bewertungszwecke beschleunigt.

Erstellen eines Aktualisierungs-Tasks

In diesem Abschnitt erstellen Sie einen Client-Task, mit dem das VirusScan-Modul und die DAT-Dateien sowie der Host Intrusion Prevention-Inhalt aktualisiert werden.

1. Wechseln Sie zu **Systeme | Systemstruktur**, und klicken Sie dann in der Menüleiste auf **Client-Tasks**.
2. Markieren Sie **Testgruppe**, und klicken Sie dann auf **Neuer Task**.
3. Geben Sie als Namen Tägliche Aktualisierung ein.
4. Wählen Sie im Dropdownmenü **Typ** den Eintrag **Aktualisieren (McAfee Agent)** aus, und klicken Sie anschließend auf **Weiter**.
5. Wählen Sie auf der Seite **Konfiguration** die Optionen **Modul**, **DAT** und **Host Intrusion Prevention-Inhalt** aus, und klicken Sie anschließend auf **Weiter**.
6. Legen Sie auf der Seite **Plan** den **Planungstyp** auf **Täglich** fest.

   HINWEIS: Beim Aktualisieren einer großen Anzahl an Systemen empfiehlt McAfee die Verwendung des Zufallsgenerators, um die Client-Abfragen zu staffeln.

7. Wählen Sie unter **Optionen** die Option **Ausgelassenen Task ausführen** aus.
8. Legen Sie für **Plan** die Einstellung **Wiederholen zwischen** fest, und stellen Sie die Zeitwerte auf **7:00**, **6:59** und **Alle 4 Stunden** ein.
9. Klicken Sie auf der Seite **Zusammenfassung** auf **Speichern**.

Die Zeitspanne für den Plan dient lediglich als Beispiel. In einer realen Umgebung werden Sie Client-Systeme wahrscheinlich so planen, dass sie über den Tag verteilt nach Aktualisierungen suchen. Mit den Planungsoptionen können Sie jeden gewünschten Plan festlegen.

Zeitweilig vom Netzwerk getrennte Systeme (z. B. Notebooks) setzen die ihnen zugewiesenen Aktualisierungs-Tasks fort. Dabei ruft das Notebook Aktualisierungen von der McAfee-Webseite (statt vom ePO-Server) ab, wenn in einem Hotel oder anderswo eine Internetverbindung verfügbar ist.

Ausbringen von McAfee Agent

McAfee Agent ist die verteilte Komponente von ePolicy Orchestrator, die auf jedem System im Netzwerk installiert werden muss, das Sie verwalten möchten. Der Agent sammelt Informationen und sendet sie an den ePO-Server. Außerdem installiert und aktualisiert er die Endpunkt-Produkte und wendet Ihre Endpunkt-Richtlinien an. Systeme können von ePolicy Orchestrator nur dann verwaltet werden, wenn McAfee Agent installiert ist.

Vor dem Ausbringen von McAfee Agent sollte die Kommunikation zwischen dem Server und den Systemen überprüft und auf das standardmäßige Administrator-Freigabeverzeichnis zugegriffen werden. Außerdem müssen Sie möglicherweise Firewall-Ausnahmen erstellen.

1 Überprüfen Sie, ob Sie Client-Systeme über deren Namen mit einem Ping-Befehl erreichen. Das bedeutet, dass der Server Client-Namen in eine IP-Adresse auflösen kann.

2 Überprüfen Sie den Zugriff auf die standardmäßige Admin$-Freigabe auf den Client-Systemen: Klicken Sie in der Windows-Benutzeroberfläche auf **Start | Ausführen**, und geben Sie dann den Befehl \\Computername\admin$ ein. Wenn die Systeme ordnungsgemäß über das Netzwerk verbunden sind, umfassen Ihre Anmeldeinformationen genügend Rechte, und der freigegebene Ordner **Admin$** ist vorhanden. Ein Dialogfeld von Windows Explorer wird geöffnet.

3 Wenn auf einem der Client-Systeme eine Firewall aktiv ist, erstellen Sie eine Ausnahme für Framepkg.exe. Das ist die Datei, die von ePolicy Orchestrator auf die zu verwaltenden Systeme kopiert wird.

Ausbringen des Agenten

Gehen Sie wie nachfolgend beschrieben vor, um McAfee Agent auf Ihre Systeme auszubringen.

1 Wechseln Sie zu **Systeme |** Systemstruktur, und klicken Sie dann in der Menüleiste auf **Systeme**.

2 Markieren Sie **Testgruppe**. Wenn diese Gruppe keine Systeme, aber Untergruppen mit Systemen enthält, klicken Sie auf das Dropdownfeld **Ebene filtern**, und wählen Sie **Diese Gruppe und alle Untergruppen** aus.

3 Wählen Sie in der Liste ein oder mehrere Systeme aus, und klicken Sie auf **Weitere Aktionen | Agenten ausbringen**.

4 Geben Sie Anmeldeinformationen ein, die über Rechte zum Installieren von Software auf Client-Systemen verfügen (z. B. ein Domänenadministrator), und klicken Sie auf **OK**.

Es dauert einige Minuten, bis McAfee Agent installiert ist und die Installationspakete für die Endpunkt-Produkte von den Client-Systemen abgerufen und ausgeführt wurden. Bei der ersten Installation legt der Agent einen zufälligen Zeitraum von 10 Minuten fest, in dem zum Abrufen von Richtlinien und Tasks eine Verbindung zu dem ePO-Server hergestellt sein muss.

Zum Ausbringen von McAfee Agent gibt es noch viele andere Möglichkeiten (siehe ePolicy Orchestrator-Dokumentation oder Online-Hilfe).

Überprüfen der Agenten-Kommunikation mit ePolicy Orchestrator

Nach der ersten Kommunikation zwischen dem Agenten und dem Server fragt der Agent den Server standardmäßig alle 60 Minuten ab. Dies wird als *Agent-zu-Server-Kommunikationsintervall* (*ASKI*) bezeichnet. Dabei ruft der Agent bei jedem Kommunikationsvorgang Richtlinienänderungen ab und erzwingt die Richtlinien lokal.

Mit dem standardmäßigen ASKI wird ein Agent, der vor 15 Minuten eine Abfrage an den Server gesendet hat, in den nächsten 45 Minuten keine neuen Richtlinien abfragen. Mit einer Agenten-Reaktivierung können Sie jedoch erzwingen, dass Systeme den Server abfragen. Eine Agenten-Reaktivierung ist nützlich, wenn Sie eine Richtlinienänderungen erzwingen müssen, bevor der nächste Kommunikationsvorgang stattfindet. Außerdem können Sie damit Clients zum Ausführen von Tasks zwingen (z. B. eine sofortige Aktualisierung).

Gehen Sie wie nachfolgend beschrieben vor, um zu überprüfen, ob Ihre Client-Systeme mit ePolicy Orchestrator kommunizieren.

1. Wechseln Sie zu **Systeme | **Systemstruktur, und klicken Sie dann in der Menüleiste auf **Systeme**.
2. Markieren Sie Ihre Gruppe **Server** oder **Workstations**.
3. Wenn eine IP-Adresse und ein Benutzername angezeigt werden, kommuniziert der Agent auf dem Client-System mit dem Server.
4. Wenn für Systeme innerhalb der nächsten fünf bis zehn Minuten keine IP-Adresse und kein Benutzername aufgeführt werden, wählen Sie **Weitere Aktionen | Agenten reaktivieren** aus.

Wenn bei einer Reaktivierung eine IP-Adresse und ein Benutzername nicht abgerufen werden kann, verhindern möglicherweise andere Faktoren in der Umgebung die Ausbringung des Agenten. In solch einem Fall können Sie das Installationsprogramm für den Agenten (Framepkg.exe) auf dem ePO-Server kopieren und auf den Client-Systemen ausführen.

Überprüfen der Client-Softwareinstallation

Je nach dem, wie viele Produkte ausgebracht sind, kann die Client-Installation einige Zeit dauern. Client-Installationen können Sie auf dem ePO-Server oder auf dem Client-System überprüfen. Klicken Sie dazu auf den Client-Systemen mit der rechten Maustaste auf das McAfee-Symbol in der Taskleiste.

Gehen Sie wie nachfolgend beschrieben vor, um Client-Installationen auf dem ePO-Server zu überprüfen.

1. Wechseln Sie zu **Systeme | **Systemstruktur, und klicken Sie dann in der Menüleiste auf **Systeme**.
2. Markieren Sie Ihre Gruppe **Server** oder **Workstations**.
3. Wählen Sie mithilfe der Kontrollkästchen einzelne Systeme aus, oder verwenden Sie die Optionen **Alle Elemente auf dieser Seite auswählen** oder **Alle Elemente auf allen Seiten auswählen**.
4. Klicken Sie auf **Weitere Aktionen | Agenten reaktivieren**.
5. Wenn Sie eine große Anzahl von Systemen reaktiviert haben, ist es hilfreich, einige Minuten zum Zufallsintervall hinzuzufügen. Klicken Sie auf **OK**.
6. Klicken Sie nach einigen Minuten auf einzelne Systeme. Auf der Seite **Systemdetails** finden Sie Informationen über das System, einschließlich der installierten McAfee-Software.

Erneutes Aufrufen der PUP-Audit-Richtlinie von VirusScan

An dieser Stelle wurden oder werden die Client-Tasks zur Softwareinstallation ausgeführt, und sämtliche Richtlinien, die Sie zuvor bereits erstellt haben, sind heruntergeladen. Wenn Sie Testsysteme mit sauberen, neu installierten Betriebssystemen verwenden, liegen möglicherweise keine PUP-Entdeckungen vor. Bei der vorliegenden Übung wird angenommen, dass auf Ihren Clients die folgenden Programme entdeckt wurden:

- Das Remote-Verwaltungstool **Tight VNC**
- Ein Port-Scanner namens **SuperScan**

Bei den meisten PUPs werden sowohl die Familie als auch der Name der Anwendung ermittelt. So wird zum Beispiel der Port-Scanner "SuperScan" als **PortScan-SuperScan** und "TightVNC" als **RemAdm-TightVNC** erkannt. Dies ist die grundsätzliche Terminologie bei der Benennung von Entdeckungen in ePO-Berichten und lokalen Client-Protokolldateien.

Gehen Sie nach Abschluss des PUP-Audits wie nachfolgend beschrieben vor, um eine neue Richtlinie zu erstellen, die auf Ihrer *Richtlinie zu unerwünschten Programmen* basiert, und erforderliche Ausschlüsse hinzuzufügen. Dabei dienen SuperScan und Tight VNC zu Beispielzwecken. Sie müssen diese Ausschlüsse nicht sofort eingeben. Sie können zu diesem Beispiel zurückkehren, wenn und falls Sie tatsächlich Ausschlüsse vornehmen müssen.

1. Wechseln Sie zu **Systeme | Systemstruktur**, und klicken Sie dann in der Menüleiste auf **Richtlinien**.
2. Wählen Sie im Dropdownmenü **Produkt** den Eintrag **VirusScan Enterprise 8.7.0** aus.
3. Markieren Sie **Testgruppe**.
4. Klicken Sie rechts neben der **Richtlinie für unerwünschte Programme** auf **Zuweisung bearbeiten**.
5. Wählen Sie **Vererbung unterbrechen und ab hier Richtlinie und Einstellungen zuweisen** aus.
6. Klicken Sie auf **Neue Richtlinie**.
7. Geben Sie einen Namen für die Richtlinie ein (z. B. PUP-Ausschlüsse für IT-Mitarbeiter, und klicken Sie auf **OK**. Der Richtlinieneditor wird geöffnet.
8. Geben Sie im Bereich **Ausschlüsse bei unerwünschten Programmen** PortScan-SuperScan ein, und klicken Sie auf das Pluszeichen (**+**) auf der rechten Seite.
9. Geben Sie RemAdm-TightVNC ein, klicken Sie noch einmal auf das Pluszeichen (**+**), und geben Sie Reg-TightVNC ein.

   Bei TightVNC ist außerdem ein "Reg"-Ausschluss für die Windows-Registrierungseinträge für diese Anwendung erforderlich. Dadurch wird der Scanner angewiesen, die zugehörigen Registrierungseinträge für diese Anwendung nicht zu säubern. Für SuperScan ist kein Reg-Ausschluss erforderlich, da es nur eine eigenständige ausführbare Datei ist.
10. Klicken Sie auf **Speichern**.
11. Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** die Richtlinie **PUP-Ausschlüsse für IT-Mitarbeiter** aus, und klicken Sie dann auf **Speichern**.

Anstatt eine ganze Kategorie zu deaktivieren ist es sicherer, nur die Tools auszuschließen, die Sie verwenden. Nehmen Sie zum Beispiel die Remote-Verwaltungstools: Sie müssen möglicherweise einige Tools für normale Vorgänge ausschließen, Sie möchten möglicherweise aber auch erfahren, ob alle nicht zugelassenen und nicht autorisierten Tools dieser Art in Ihrem Netzwerk vom McAfee AntiSpyware-Modul gefunden werden.

Nach Abschluss des PUP-Audits müssen Sie unbedingt die VirusScan-Einstellung wieder zurück auf **Säubern** setzen und eine Richtlinie mit Ausschlüssen erstellen. Wenn Sie die Richtlinie nicht wieder so zurücksetzen, dass sie PUPs säubert, wird Spyware nicht entfernt werden.

Zurücksetzen der On-Access-Scan-Richtlinie

In einem früheren Schritt haben Sie eine neue Richtlinie erstellt, mit der der On-Access-Scanner angewiesen wird, PUPs zu entdecken, aber nicht zu säubern. Gehen Sie wie nachfolgend beschrieben vor, um die standardmäßige Scanner-Richtlinie erneut anzuwenden, die das Säubern aktiviert.

1 Wechseln Sie zu **Systeme | Systemstruktur**, und klicken Sie dann in der Menüleiste auf **Richtlinien**.
2 Wählen Sie im Dropdownmenü **Produkt** den Eintrag **VirusScan Enterprise 8.7.0** aus.
3 Markieren Sie **Testgruppe**.
4 Klicken Sie rechts neben **Richtlinien bei Zugriff für Standardvorgänge** auf **Zuweisung bearbeiten**.
5 Wählen Sie im Dropdownmenü **Zugewiesene Richtlinie** den Eintrag **My Default** aus.
6 Aktivieren Sie das Optionsfeld für die PUPs-Audit-Richtlinie, die je nach den zuvor vorgenommenen Einstellungen **Globaler Stamm** oder **Eigene Organisation** lautet.
7 Klicken Sie auf **Speichern**.

Überprüfen des On-Demand-Scan-Tasks

In einer bereits durchgeführten Übung haben Sie einen regelmäßigen Scan-Task für das Client-System geplant. Im Rahmen jener Konfiguration wurde der Scanner angewiesen, PUPs zeitweise nur zu entdecken, aber nicht zu säubern. Gehen Sie wie nachfolgend beschrieben vor, um die Option zurückzusetzen, die das Säubern während eines geplanten Scans aktiviert.

1 Wechseln Sie zu **Systeme | Systemstruktur**, und klicken Sie dann in der Menüleiste auf **Client-Tasks**.
2 Markieren Sie **Testgruppe**.
3 Suchen Sie den von Ihnen erstellten Scan-Task, und klicken Sie dann in der Spalte **Aktionen** auf **Bearbeiten**.
4 Klicken Sie auf der ersten Seite des Assistenten auf **Weiter**.
5 Klicken Sie auf der Seite **Konfiguration** auf **Aktionen**, und wählen Sie dann im Dropdownmenü **Wenn ein unerwünschtes Programm gefunden wird** den Eintrag **Dateien säubern** aus.
6 Klicken Sie auf **Speichern**.

VirusScan säubert nun alle PUPs, die Sie nicht explizit ausgeschlossenen haben. Wenn die Client-Systeme den Server das nächste Mal abfragen, laden sie Ihre Konfigurationsänderungen herunter.

Verwenden von Dashboards und Abfragen

Dashboards und Abfragen stellen verschiedene Typen von Statusinformationen über Ihre Umgebung zur Verfügung. Jedes Produkt in der Total Protection for Endpoint-Suite beinhaltet vordefinierte Abfragen. Die Suite umfasst auch einige vordefinierte Dashboards. Außerdem können Sie eigene benutzerdefinierte Dashboards und Abfragen erstellen.

Standardmäßig ist nach der Installation das Dashboard "ePO-Zusammenfassung" das einzige aktive Dashboard. In diesem Abschnitt aktivieren Sie ein zweites Dashboard, ändern eine der Überwachungen, führen eine vordefinierte Abfrage aus und erstellen eine benutzerdefinierte Abfrage.

Aktivieren eines Dashboards

Damit ein Dashboard auf der Seite **Dashboards** zum aktiven Set in der Registerkartenleiste gehört, müssen Sie es aktivieren.

1. Wechseln Sie zu Dashboards, klicken Sie auf **Optionen**, und wählen Sie dann **Eigene Dashboards verwalten** aus. Die Seite **Dashboards verwalten** wird angezeigt.
2. Markieren Sie in der Liste **Dashboards** den Eintrag **HIP-Dashboard**, und klicken Sie anschließend auf **Aktivieren**.
3. Wenn Sie dazu aufgefordert werden, klicken Sie zunächst auf **OK** und dann auf **Schließen**.

Das HIP-Dashboard wird jetzt in der Registerkartenleiste angezeigt. Schauen Sie sich dieses Dashboard und die darin bereitgestellten Informationen in Ruhe an.

Ändern einer Dashboard-Überwachung

Die meisten Standard-Dashboards enthalten sechs Überwachungen. Wenn die Standardüberwachungen nicht die gewünschten Informationen liefern, können Sie den Satz von Überwachungen ändern, statt ein neues Dashboard zu erstellen. Zum Anzeigen von Informationen zu VirusScan Enterprise und potenziell unerwünschten Programmen müssen Sie das Dashboard **VSE: Aktuelle Entdeckungen** erst duplizieren und anschließend ändern.

1. Wechseln Sie zu Dashboards, klicken Sie auf **Optionen**, und wählen Sie dann **Eigene Dashboards verwalten** aus. Die Seite **Dashboards verwalten** wird angezeigt.
2. Markieren Sie in der Liste **Dashboards** den Eintrag **VSE: Aktuelle Entdeckungen**, und klicken Sie dann auf **Duplizieren**.
3. Geben Sie bei **Name** VSE: Entdeckungen (benutzerdefiniert) ein, und klicken Sie dann auf **OK**.
4. Klicken Sie auf **Bearbeiten**.
5. Suchen Sie die Überwachung mit dem Namen **VSE: In den letzten 24 Stunden entdeckte Bedrohungen**, und klicken Sie auf **Löschen**.
6. Klicken Sie auf **Neue Überwachung**.
7. Wählen Sie in der Liste **Kategorie** den Eintrag **Abfragen** aus.
8. Wählen Sie in der Liste **Überwachung** den Eintrag **VSE: DAT-Ausbringung** aus, und klicken Sie dann auf **OK**.

9 Suchen Sie die Überwachung mit dem Namen **VSE: In den letzten 7 Tagen entdeckte Bedrohungen**, und klicken Sie auf **Löschen**.
10 Klicken Sie auf **Neue Überwachung**.
11 Wählen Sie in der Liste **Kategorie** den Eintrag **Abfragen** aus.
12 Wählen Sie in der Liste **Überwachung** den Eintrag **VSE: Am häufigsten verletzte Zugriffsschutzregeln** aus, und klicken Sie dann auf **OK**.
13 Klicken Sie auf **Speichern**.
14 Klicken Sie zunächst auf **Aktivieren** und dann auf **OK**.
15 Klicken Sie auf **Schließen**.
16 Klicken Sie in der Registerkartenleiste **Dashboards** auf **VSE: Entdeckungen (benutzerdefiniert)**.

Die beiden hinzugefügten Überwachungen zeigen ein Kreisdiagramm (DAT-Ausbringung) und eine Übersichtstabelle (Am häufigsten verletzte Zugriffsschutzregeln) an. Berücksichtigen Sie beim Erstellen Ihrer eigenen Abfragen den Typ der Daten, die Sie anzeigen möchten, und die Art der Anzeige.

Ausführen einer vordefinierten Abfrage

Wie aus dem vorherigen Schritt ersichtlich, können Abfragen die von Dashboard-Überwachungen angezeigten Quelldaten sein. Sie können Abfragen auch einzeln ausführen.

Zum Überprüfen der Installation von VirusScan Enterprise auf Ihren Client-Systemen können Sie die Abfrage **VSE: Konformität von Version 8.7** ausführen.

1 Wechseln Sie zu **Berichterstellung |** Abfragen.
2 Markieren Sie in der Liste **Abfragen** den Eintrag **VSE: Konformität von Version 8.7**.
3 Klicken Sie auf **Ausführen**.

In einem Kreisdiagramm wird angezeigt, ob die Systeme konform oder nicht konform sind. Die Konformität wird in der Abfrage durch folgende Kriterien festgelegt:

- VirusScan® Enterprise 8.7i ist installiert.
- Die Version des Scan-Moduls ist mindestens 5200.
- Die Antiviren-Signaturdatei (DAT) auf dem Client unterscheidet sich höchstens um 3 Versionen von der im ePO-Master-Repository.

Wenn eines dieser Kriterien nicht erfüllt wird, kann ein System als nicht konform bezeichnet werden. Genauere Informationen zu einigen Kriterien, z. B. den DAT-Versionen auf verschiedenen Clients, erhalten Sie durch Ausführen der Abfrage **VSE: DAT-Ausbringung**.

Zum Überprüfen, ob Host Intrusion Prevention mit der richtigen Version installiert ist, können Sie die Abfrage **HIP: Client-Versionen** ausführen. Wenn Sie überprüfen möchten, ob diese Clients über die neuesten Aktualisierungen verfügen, können Sie die Abfrage **HIP: Content-Versionen** ausführen. Sie können diese Abfragen auch als Dashboard-Überwachungen hinzufügen.

Erstellen einer benutzerdefinierten Abfrage

Gehen Sie wie nachfolgend beschrieben vor, um eine Abfrage zu erstellen, die alle PUP-Entdeckungen anzeigt.

1 Wechseln Sie zu **Berichterstellung |** Abfragen.
2 Klicken Sie auf **Neue Abfrage**.
3 Wählen Sie in der Liste den Eintrag **Ereignisse** aus, und klicken Sie dann auf **Weiter**.

4 Wählen Sie Folgendes aus, und klicken Sie anschließend auf **Weiter**:

Element	**Auszuwählende Option**
Ergebnisse anzeigen als	**Balkendiagramm**
Mögliche Balkenbeschriftungen	**Name der Bedrohung**
Mögliche Balkenwerte	**Anzahl der Ereignisse**

5 Klicken Sie erneut auf **Weiter**, um die Seite **Spalten** zu umgehen.

6 Gehen Sie auf der Seite **Filter** im Abschnitt **Ereignisse** unter **Verfügbare Eigenschaften** folgendermaßen vor:

- Klicken Sie auf **Name des entdeckenden Produkts**, und legen Sie für **Vergleich** die Einstellung **Ist gleich** fest. Geben Sie für **Wert** VirusScan Enterprise 8.7 ein.
- Klicken Sie auf **Ereignis-ID**, und legen Sie für **Vergleich** die Einstellung **Größer als** fest. Geben Sie für **Wert** 20000 ein.
- Klicken Sie auf **Name der Bedrohung**, und legen Sie für **Vergleich** die Einstellung **Enthält nicht** fest. Geben Sie für **Wert** Cookie ein.

7 Klicken Sie auf **Ausführen**.

8 Klicken Sie nach dem Anzeigen der Ergebnisse auf **Speichern**. Geben Sie dann als Namen der Abfrage VSE: Alle PUP-Entdeckungen ein, und klicken Sie dann auf **Speichern**.

Wenn Sie eine benutzerdefinierte Abfrage speichern, wird diese in alphabetischer Reihenfolge in die Liste aller Abfragen aufgenommen. Sie können diese Abfrage nun jederzeit ausführen oder als Dashboard-Überwachung verwenden. Wenn Sie spezielle Zeiträume für PUP-Entdeckungen festlegen möchten, können Sie diese Abfrage duplizieren und die Eigenschaft **Zeit der Ereignisgenerierung** als zusätzlichen Filter hinzufügen.

Zusammenfassung

Herzlichen Glückwunsch! Nach Abschluss der Anleitungen dieses Handbuchs haben Sie viele der typischen Aufgaben durchgeführt, die beim Erstellen und Warten einer sicheren Netzwerkumgebung anfallen.

Sie haben Folgendes durchgeführt:

1. Sie haben die Total Protection for Endpoint-Suite installiert.
2. Sie haben einen Task aktiviert und ausgeführt, der das ePO-Master-Repository von der McAfee-Webseite aus aktualisiert.
3. Sie haben eine Systemstruktur erstellt und Testsysteme in Gruppen hinzugefügt.
4. Sie haben eine neue McAfee Agent-Richtlinie erstellt und übernommen, die auf verwalteten Systemen das Agenten-Symbol in der Taskleiste anzeigt.
5. Sie haben neue Richtlinien für Endpunkt-Produkte erstellt und übernommen. Dazu gehören Folgende:
    - Verschiedene VirusScan-Richtlinien, einschließlich einer Richtlinie für zum Durchführen eines Audits nach PUPs.
    - Eine SiteAdvisor Enterprise Plus-Richtlinie.
    - Eine Host Intrusion Prevention-Richtlinie.
6. Sie haben einen Ausbringungs-Task erstellt, um VirusScan, Host Intrusion Prevention und SiteAdvisor Plus auf den Client-Systemen zu installieren.
7. Sie haben Richtlinien für den E-Mail-Schutz erstellt und übernommen.
8. Sie haben einen Client-Aktualisierungs-Task erstellt, der die Clients auf dem aktuellen Stand hält.
9. Sie haben McAfee Agent ausgebracht.
10. Sie haben die Agent-zu-Server-Kommunikation überprüft und Agenten-Reaktivierungen gesendet, um sicherzustellen, dass Ihre verwalteten Systeme die neuen Richtlinien empfangen haben.
11. Sie haben die PUP-Audit-Richtlinie um Ausschlüsse ergänzt.
12. Sie haben die standardmäßige On-Access-Scan-Richtlinie neu übernommen und den On-Demand-Scan-Task zum Säubern von PUPs zurückgesetzt.
13. Sie haben ein zweites Dashboard aktiviert, Überwachungen auf einem Dashboard geändert und eine vordefinierte Abfrage ausgeführt.
14. Sie haben eine benutzerdefinierte Abfrage zum Auflisten von PUP-Entdeckungen erstellt.

Verweise

Unter den in diesem Abschnitt aufgeführten Links können Sie auf weitere Informationen zugreifen.

Unterstützung durch Lesen

Durchsuchen Sie die preisgekrönte KnowledgeBase von McAfee nach Antworten auf Ihre Fragen.

Durchsuchen Sie die KnowledgeBase.

Weitere Informationen zu Total Protection for Endpoint finden Sie in den folgenden Produktdokumentationen:

ePolicy Orchestrator 4.0

- ePolicy Orchestrator 4.0 – Handbuch zur Testversion
- ePolicy Orchestrator 4.0.2 – Produkthandbuch
- ePolicy Orchestrator 4.0 – Installationshandbuch
- ePolicy Orchestrator 4.0 – Handbuch zur Hardwaredimensionierung und Bandbreitennutzung
- ePolicy Orchestrator 4.0 – Kurzanleitung
- ePolicy Orchestrator 4.0 – Verwenden von Protokolldateien zur Fehlerbehebung
- ePolicy Orchestrator 4.0 – Hauptliste mit Supportartikeln zu dieser Version

VirusScan Enterprise 8.7i

- VirusScan Enterprise 8.7i – Installationshandbuch
- VirusScan Enterprise 8.7i – Produkthandbuch
- VirusScan Enterprise 8.7i – Kurzanleitung
- Access Protection in McAfee VirusScan Enterprise and Host Intrusion Prevention (Zugriffsschutz in McAfee VirusScan Enterprise und Host Intrusion Prevention) – Whitepaper

AntiSpyware Enterprise 8.7

- AntiSpyware Enterprise-Modul 8.7 – Produkthandbuch
- AntiSpyware Enterprise 8.7 – Versionshinweise

McAfee Host Intrusion Prevention 7.0

- Host Intrusion Prevention 7.0.0 – Installationshandbuch
- Adopting Host Intrusion Prevention - Best practices for quick success (Einsatz von McAfee Host IPS: Der einfachste Weg zum Erfolg)
- Host Intrusion Prevention 7.0.0 für ePO 4.0 – Produkthandbuch
- Host Intrusion Prevention 7.0 Firewall Protocol Support (Host Intrusion Prevention 7.0 – Unterstützung für das Firewallprotokoll)

- Host Intrusion Prevention 7.x Multi-Slot Policies and their Effective Policy (Host Intrusion Prevention 7.x – Richtlinien für mehrere Slots und deren wirksame Richtlinie)
- Host Intrusion Prevention Firewall: Connection-Aware Groups (Host Intrusion Prevention-Firewall: Verbindungsabhängige Gruppen)
- Host Intrusion Prevention 7.x Adaptive Mode (Host Intrusion Prevention 7.x – Adaptiver Modus)
- Access Protection in McAfee VirusScan Enterprise and Host Intrusion Prevention (Zugriffsschutz in McAfee VirusScan Enterprise und Host Intrusion Prevention) – Whitepaper

SiteAdvisor Enterprise Plus 2.0

- SiteAdvisor Enterprise Plus 2.0 – Produkthandbuch
- Mapping the mal web, Revisited (Das aktuelle böswillige Web – Update) – Whitepaper
- Prevention is the best medicine (Vorsorge ist die beste Medizin) – Whitepaper
- McAfee SECURE™ shopping portal (McAfee SECURE™-Einkaufsportal)
- Ressourcen für Website-Eigentümer und Verbraucher

GroupShield 7.0 for Microsoft Exchange

- GroupShield 7.0.1 for Microsoft Exchange – Handbuch zu empfohlenen Vorgehensweisen
- GroupShield 7.0 for Microsoft Exchange – Benutzerhandbuch
- GroupShield 7.0.1 for Microsoft Exchange – Nachtrag zum Benutzerhandbuch

GroupShield 7.0 for Lotus Domino

- GroupShield 7.0 for Lotus Domino – ePolicy Orchestrator – Konfigurationshandbuch
- GroupShield 7.0 for Lotus Domino – Installationshandbuch
- GroupShield 7.0 for Lotus Domino – Produkthandbuch
- GroupShield 7.0 for Lotus Domino – Handbuch zu empfohlenen Vorgehensweisen

Unterstützung durch Sehen

Zeigen Sie Lernprogramme an.

Sehen Sie sich Lernprogramme an, die häufige Probleme und Fragen behandeln.

Unterstützung durch Handeln

Laden Sie Software-Aktualisierungen herunter.

Rufen Sie die neuesten Antiviren-Definitionen, Sicherheitsaktualisierungen und Produktversionen ab. Für Produktpatches und Wartungsversionen müssen Sie sich am ServicePortal anmelden.

Global Support Lab

Konfigurieren und analysieren Sie häufige Probleme in einer funktionierenden Testumgebung.